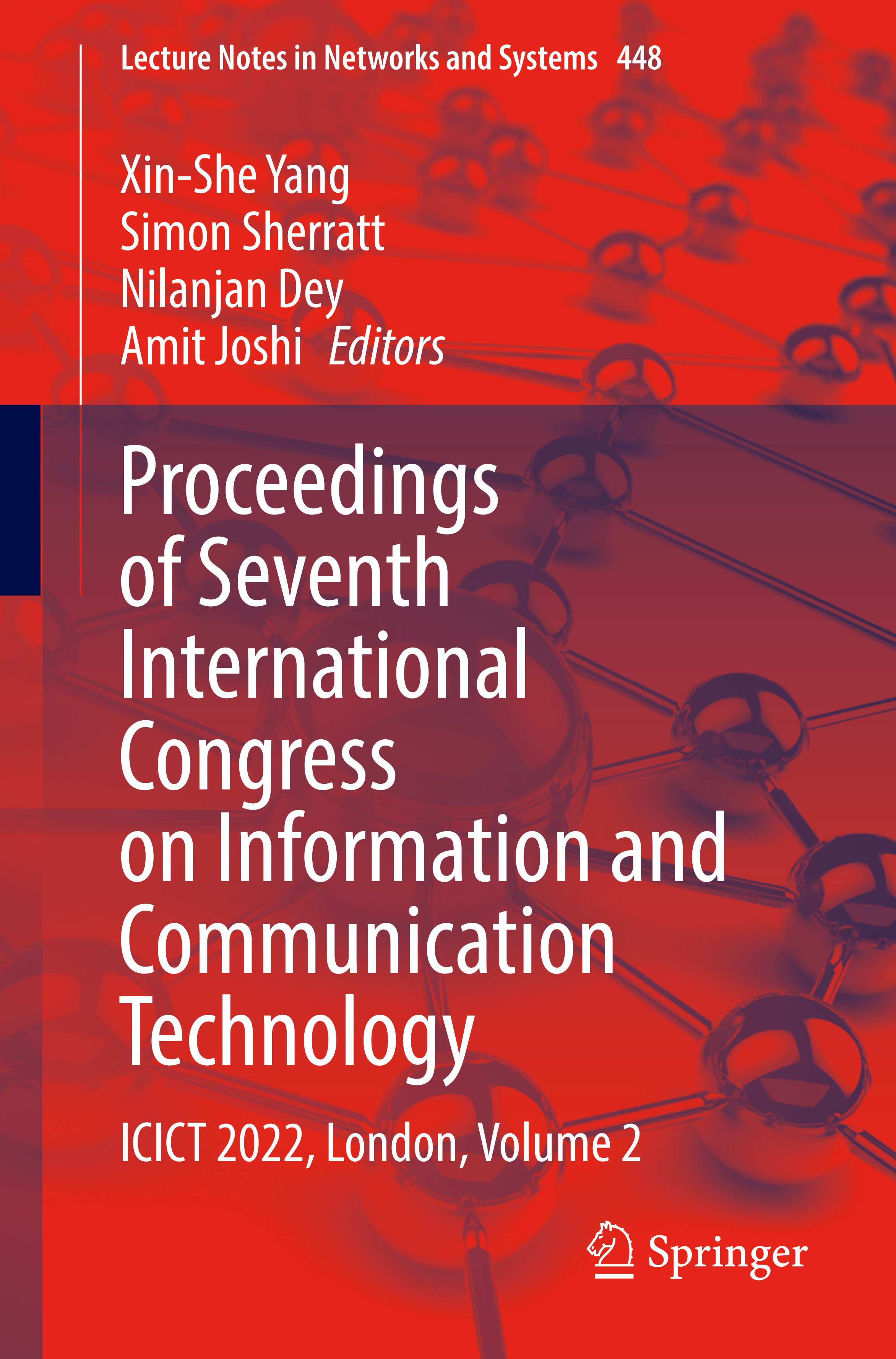
Lecture Notes in Networks and Systems 448

Xin-She Yang
Simon Sherratt
Nilanjan Dey
Amit Joshi *Editors*

Proceedings of Seventh International Congress on Information and Communication Technology

ICICT 2022, London, Volume 2



Springer

Lecture Notes in Networks and Systems

Volume 448

Xin-She Yang · Simon Sherratt · Nilanjan Dey ·
Amit Joshi
Editors

Proceedings of Seventh International Congress on Information and Communication Technology

ICICT 2022, London, Volume 2

Springer

Editors

Xin-She Yang
Middlesex University
London, UK

Simon Sherratt
The University of Reading
Reading, UK

Nilanjan Dey
JIS University
Kolkata, India

Amit Joshi
Global Knowledge Research Foundation
Ahmedabad, India

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-19-1609-0 ISBN 978-981-19-1610-6 (eBook)
https://doi.org/10.1007/978-981-19-1610-6

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The Seventh International Congress on Information and Communication Technology will be held during 21–24 February 2022 in a hybrid mode and organised by Global Knowledge Research Foundation. The associated partners were Springer and InterYIT IFIP, Activate Learning, City of Oxford College, UK. The conference will provide a useful and wide platform both for display of the latest research and for exchange of research results and thoughts. The participants of the conference will be from almost every part of the world, with backgrounds of either academia or industry, allowing a real multinational multicultural exchange of experiences and ideas.

A great pool of more than 1100 papers were received for this conference from across 95 countries among which around 300 papers were accepted and will be presented through digital platforms during the two days. Due to the overwhelming response, we had to drop many papers in the hierarchy of the quality. Total 42 technical sessions will be organised in parallel in 4 days along with a few keynotes and panel discussions in hybrid mode. The conference will be involved in deep discussion and issues which will be intended to solve at global levels. New technologies will be proposed, experiences will be shared, and future solutions for design infrastructure for ICT will also be discussed. The final papers will be published in four volumes of proceedings by Springer LNNS Series.

Over the years, this congress has been organised and conceptualised with collective efforts of a large number of individuals. I would like to thank each of the committee members and the reviewers for their excellent work in reviewing the papers. Grateful acknowledgements are extended to the team of Global Knowledge Research Foundation for their valuable efforts and support.

I look forward to welcoming you to the 7th Edition of this ICICT Congress 2022.

Amit Joshi, Ph.D.
Organising Secretary, ICICT 2022
Director—Global Knowledge Research Foundation
Ahmedabad, India

Contents

Editors and Contributors

About the Editors

Xin-She Yang obtained his D.Phil. in Applied Mathematics from the University of Oxford, and subsequently worked at the Cambridge University and the National Physical Laboratory (UK) as Senior Research Scientist. He is currently Reader in Modeling and Optimization at Middlesex University London and Adjunct Professor at Reykjavik University (Iceland). He is also elected Bye-Fellow at the Cambridge University and IEEE CIS Chair for the Task Force on Business Intelligence and Knowledge Management. He was included in the "2016 Thomson Reuters Highly Cited Researchers" list.

Simon Sherratt was born near Liverpool, England, in 1969. He is currently Professor of Biosensors in the Department of Biomedical Engineering, University of Reading, UK. His main research area is signal processing and personal communications in consumer devices, focusing on wearable devices and health care. He received the 1st place IEEE Chester Sall Memorial Award in 2006, the 2nd place in 2016 and the 3rd place in 2017.

Nilanjan Dey is Assistant Professor in the Department of Information Technology, Techno India College of Technology, India. He has authored/edited more than 75 books with Springer, Elsevier, Wiley, CRC Press and published more than 300 peer-reviewed research papers. He is Editor-in-Chief of the International Journal of Ambient Computing and Intelligence; Series Co-editor of Springer Tracts in Nature-Inspired Computing (STNIC); and Series Co-editor of Advances in Ubiquitous Sensing Applications for Healthcare, Elsevier.

Amit Joshi is currently Director of Global Knowledge Research Foundation and also Entrepreneur and Researcher who has completed his masters and research in the areas of cloud computing and cryptography in medical imaging. He has an experience of around 10 years in academic and industry in prestigious organizations. He is an active member of ACM, IEEE, CSI, AMIE, IACSIT-Singapore, IDES, ACEEE, NPA and many other professional societies. Currently, he is International Chair of InterYIT at International Federation of Information Processing (IFIP, Austria), He has presented and published more than 50 papers in national and international journals/conferences of IEEE and ACM. He has also edited more than 40 books which are published by Springer, ACM and other reputed publishers. He has also organized more than 50 national and international conferences and programs in association with ACM, Springer, IEEE to name a few across different countries including India, UK, Europe, USA, Canada, Thailand, Egypt and many more.

Contributors

Zaid Ameen Abduljabbar Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq;
Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen, China

Dm. Mehedi Hasan Abid Daffodil International University, Dhaka, Bangladesh

Rizal Tjut Adek Department of Informatics, Universitas Malikussaleh Aceh, Aceh, Indonesia

Ammad Adil COMSATS University Islamabad, Islamabad, Pakistan

Camila Z. Aguiar Innovation Laboratory-LINO, Institute of Information and Communication Technology of Espírito Santo, Vitória, Brazil

Eisler Aguilar Department of Electronic and Circuits, Universidad Simón Bolívar, Caracas, Venezuela

Saahira Ahamed Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia

Sampson Akwafuo California State University, Fullerton, CA, USA

Rasha Al Bashaireh Tafila Technical University, Tafila, Jordan

Mustafa A. Al Sibahee College of Big Data and Internet, Shenzhen Technology University, Shenzhen, China;
Computer Technology Engineering Department, Iraq University College, Basrah, Iraq

Zuhoor Al-Khanjari Department of Computer Science, College of Science, Sultan Qaboos University, Muscut, Sultanate of Oman

Iman Al-Kindi Department of Computer Science, College of Science, Sultan Qaboos University, Muscut, Sultanate of Oman

Abdulrahman Alamer Department of Information Technology and Security, Jazan University, Jazan, Saudi Arabia

Raul Albertti Alumbra.ai, Santiago de Chile, Chile

Hakim Allali FST, LAVETE Laboratory, Hassan First University of Settat, Settat, Morocco

Tatiana Allik Doctor Music From Estonia" OÜ, Kohtla-Järve, Estonia

Ziad Almtiri Department of Management Information Systems, Taif University, Taif, Saudi Arabia;
Newcastle Business School, University of Newcastle, Callaghan, NSW, Australia

Sandra Rodriguez Álvarez University Corporation Comfacauca-Unicomfacauca, Popayán, Colombia

Jim Alves-Foss Center for Secure and Dependable Systems, University of Idaho, Moscow, ID, USA

Abhineet Anand Chitkara University Institute of Engineering and Technology, Punjab, India

Vassiliki Andronikou School of Electrical and Computer Engineering, National Technical University, Athens, Greece

Nguyen Xuan Anh Institute of Geophysics, Vietnam Academy of Science and Technology, Cau Giay, Hà Noi, Vietnam

Aziz Anouar ENSAM RABAT, Mohammed V University, Rabat, Morocco

Carlos E. Arellano-Ramírez Universidad Nacional de Piura, Piura, Peru

Md. Assaduzzaman Daffodil International University, Dhaka, Bangladesh

Saidatunnajwa Abdul Aziz Universiti Kuala Lumpur, Kuala Lumpur, Malaysia

Abdelghani Azri FST, LAVETE Laboratory, Hassan First University of Settat, Settat, Morocco

Milian Badea Transilvania University of Brasov, Brasov, Romania

Khaled Badran Department of Computer Engineering, Military Technical College, Cairo, Egypt

Abhijeet Singh Bais Department of CS & IT, IIS (Deemed To Be University), Jaipur, India

Awatef Salem Balobaid Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia

Jeremy Barnett The Bartlett, University College London, London, UK

Sultan Basudan Department of Information Technology and Security, Jazan University, Jazan, Saudi Arabia

Filip Begiełło Smart Geometries Sp. z o.o., Warszawa, Poland

Driss Belghyti Faculty of Science, Laboratory: Natural Resources and Sustainable Development, Ibn Tofail University, Kenitra, Morocco

Abdelfatah Benchahid Faculty of Science, Laboratory: Natural Resources and Sustainable Development, Ibn Tofail University, Kenitra, Morocco

Mohammed Bennani ENSAM RABAT, Mohammed V University, Rabat, Morocco

Anas Benslimane Laboratory Renewable Energy, Embedded System and Information Processing, National School of Applied Sciences, University of Mohammed I, Oujda, Morocco

Belen Bermejo Computer Science Department, University of the Balearic Islands, Palma, Spain

Uliane B. Bernadino Innovation Laboratory-LINO, Institute of Information and Communication Technology of Espírito Santo, Vitória, Brazil

Ekkarat Boonchieng Department of Computer Science and Graduate School, Faculty of Science, Chiang Mai University, Chiang Mai, Thailand;
Department of Computer Science and Data Science Research Center, Faculty of Science, Chiang Mai University, Chiang Mai, Thailand

Waraporn Boonchieng Faculty of Public Health, Chiang Mai University, Chiang Mai, Thailand

Jamal Bouchnaif Laboratory of Electrical Engineering and Maintenance (LEEM), BP: 473 Higher School of Technology, University of Mohammed I, Oujda, Morocco

M. A. Bucarelli Department of Astronautics, Electric and Energy Engineering, Sapienza University of Rome, Rome, Italy

Bustami Bustami Department of Informatics, Universitas Malikussaleh Aceh, Aceh, Indonesia

Tomasz Bławucki Smart Geometries Sp. z o.o., Warszawa, Poland

Michael Cabanillas-Carbonell Universidad Privada del Norte, Lima, Perú

Maria Fernanda Cabrera-Umpierrez Universidad Politécnica de Madrid, Madrid, Spain

Gülay Canbaloğlu Delft University of Technology, Center for Safety in Healthcare, Delft, The Netherlands;
Department of Computer Engineering, Koç University, Istanbul, Turkey

Jean Pierre Cances XLIM Research Institute, UMR CNRS 7252, Limoges, France

Andrea Carboni National Research Council, Institute of Information Science and Technologies, Pisa, Italy

F. Carere Department of Astronautics, Electric and Energy Engineering, Sapienza University of Rome, Rome, Italy

Martin Carnier Alumbra.ai, Santiago de Chile, Chile

Steven Castro Universidad Politécnica Salesiana, Quito, Ecuador; Universidad Politécnica de Madrid, Madrid, España

Zheng Chen Nara Institute of Science and Technology, Ikoma, Nara, Japan

Baldreck Chipangura University of South Africa, UNISA, Pretoria, South Africa

HeeSeok Choi ATGLab R&D Center, Seoul, Korea

Kwang Sik Chung Department of Computer Science, Korea National Open University, Seoul, Korea

António Leça Coelho Laboratório Nacional de Engenharia Civil, Lisboa, Portugal

Francesco Colace DIIN University of Salerno, Fisciano, Italy

Dajana Conte DIPMAT University of Salerno, Fisciano, Italy

Fabien Courreges XLIM Research Institute, UMR CNRS 7252, Limoges, France

B. Cynddia Department of CSE, Shiv Nadar University, Chennai, India

Lucia de Espona FHNW University of Applied Arts and Sciences Northwestern Switzerland, School of Business, Institute for Information Systems, Olten, Switzerland

J. Dell'Olmo Department of Astronautics, Electric and Energy Engineering, Sapienza University of Rome, Rome, Italy

Alexander Demidovskij Higher School of Economics, Nizhny Novgorod, Russia; Intel Corporation, Nizhny Novgorod, Russia

Ketan Sanjay Desale Pimpri Chinchwad College of Engineering, Pune, India

Luh Joni Erawati Dewi Universitas Pendidikan Ganesha, Singaraja, Bali, Indonesia

Qiang Duan Inspur Academy of Science and Technology, Jinan, Shandong, China

Valentin Egger Research group ROADMAP-5G, Carinthia University of Applied Sciences, Klagenfurt, Austria

Khadija El Kharrim Faculty of Science, Laboratory: Natural Resources and Sustainable Development, Ibn Tofail University, Kenitra, Morocco

Hossam Elzayady Department of Computer Engineering, Military Technical College, Cairo, Egypt

Natalya Eremina Academy of Rehabilitation Medicine, Clinical Psychology, and Music Therapy LLC, Moscow, Russia

Alexei Ermakov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

Muhammad Farrukh FAST-NUCES University, Karachi, Pakistan

Mikhail Fedorov Intel Corporation, Nizhny Novgorod, Russia

Daniel A. Flores-Córdova Universidad Nacional de Piura, Piura, Peru

Vasileios Galafagas General Evening High School of Volos, Volos, Greece

Victor Garcia-Rios Universidad Autónoma del Perú, Lima, Perú

F. M. Gatta Department of Astronautics, Electric and Energy Engineering, Sapienza University of Rome, Rome, Italy

Liliana Gavidia Engineering, Science and Technology School, Universidad Internacional de Valencia, Valencia, Spain

I. Gede Aris Gunadi Universitas Pendidikan Ganesha, Singaraja, Bali, Indonesia

A. Geri Department of Astronautics, Electric and Energy Engineering, Sapienza University of Rome, Rome, Italy

Hossein Ghodosi James Cook University, Townsville, QLD, Australia

Fotios Gioulekas Directorate of Informatics, 5th Regional Health Authority, Larissa, Greece

Praveetha Gobinathan Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia

Clara Lucía Burbano González Mayor University, Santiago, Chile

Ramiro Gonçalves UTAD (Universidade de Trás-os-Montes e Alto Douro), Vila Real, Portugal

Yury Gorbachev Intel Corporation, Nizhny Novgorod, Russia

Brij Gupta International Center for AI and Cyber Security Research and Innovations, Asia University, Taichung, Taiwan

Adil Haddi ENSA, LAVETE Laboratory, Hassan First University of Settat, Berrechid, Morocco

N. Hadifar Department of Astronautics, Electric and Energy Engineering, Sapienza University of Rome, Rome, Italy

Tzipora Halevi Department of Computer Science, Brooklyn College, City University of New York, NY, USA

Amirreza Hamidi James Cook University, Townsville, QLD, Australia

Ying Han School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China

Md Rashedul Hasan Cybertrendz Inc., Dhaka, Bangladesh

David Helbert XLIM Research Institute, UMR CNRS 7252, Limoges, France

Micha Helbig Volkswagen AG, Wolfsburg, Germany

Jens Hoedt Volkswagen AG, Wolfsburg, Germany

Kurt Horvath Research group ROADMAP-5G, Carinthia University of Applied Sciences, Klagenfurt, Austria

Syed Akhter Hossain Daffodil International University, Dhaka, Bangladesh

Gede Indrawan Universitas Pendidikan Ganesha, Singaraja, Bali, Indonesia

Robert Ipanaqué-Chero Universidad Nacional de Piura, Piura, Peru

Tariqul Islam Daffodil International University, Dhaka, Bangladesh

Ivan Ivanchev University of Architecture, Civil Engineering and Geodesy (UACEG), Sofia, Bulgaria

Jhonattan Iñacasha Universidad Politécnica Salesiana, Quito, Ecuador;
Universidad Politécnica de Madrid, Madrid, España

Md. Ismail Jabiullah Daffodil International University, Dhaka, Bangladesh

Kai Jiang Inspur Academy of Science and Technology, Jinan, Shandong, China

Mengmeng Jiang Inspur Academy of Science and Technology, Jinan, Shandong, China

Zhihang Jiang Inspur Academy of Science and Technology, Jinan, Shandong, China

Judith K. Jiménez-Vilcherrez Universidad Tecnológica del Perú, Piura, Peru

Weiduo Jin Inspur International Limited, Jinan, Shandong, China

Nur Jannah Johari Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, Malaysia

Carlos Juiz Computer Science Department, University of the Balearic Islands, Palma, Spain

Kamalia Azma Kamaruddin Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, Malaysia

Efstathios Karanastasis School of Electrical and Computer Engineering, National Technical University, Athens, Greece

Panagiotis Katsaros Department of Informatics, Aristotle University of Thessaloniki, Thessaloniki, Greece

Asma Khan NED, University, Karachi, Pakistan

Sadia Khan COMSATS University Islamabad, Islamabad, Pakistan

Tariq Jamil Saifullah Khanzada Mehran University of Engineering and Technology, Jamshoro, Pakistan;
King Abdul Aziz University, Jeddah, Saudi Arabia

Galia Kondova School of Business FHNW, Basel, Switzerland

Ulrich Konigorski Technische Universität Darmstadt, Darmstadt, Germany

Sergei Kozhevnikov CIIRC, Czech Technical University in Prague, Prague 6, Czech Republic

S. Krishnakumar Department of IST, Anna University, Chennai, India

Snehal Kullolli Pimpri Chinchwad College of Engineering, Pune, India

Ajay Kumar Chitkara University Institute of Engineering and Technology, Punjab, India

Anjali Kurhade Pimpri Chinchwad College of Engineering, Pune, India

Alexandra La Cruz Engineering Faculty, Universidad de Ibagué, Tolima, Colombia

Omar Lahlou Services of the Prefectural Ambulatory Action Infrastructures, Kenitra, Morocco

Abdelhak Lamreoua Laboratory of Electrical Engineering and Maintenance (LEEM), BP: 473 Higher School of Technology, University of Mohammed I, Oujda, Morocco

Frédéric Lardeux LERIA, SFR MATHSTIC, Univ Angers, Angers, France

Miguel Ángel castillo Leiva Mayor University, Santiago, Chile

Ruth G. Lennon Letterkenny Institute of Technology, Letterkenny, Ireland

Rui Li Inspur Academy of Science and Technology, Jinan, Shandong, China

Vincent Li Western Connecticut State University, Danbury, CT, USA;
Horace Mann School, Bronx, NY, USA

Wei Li Inspur Academy of Science and Technology, Jinan, Shandong, China

Yunhan Li Yiwu Industrial & Commercial College, Yiwu, China

Frederic Lievens Lievens-Lanckman Bvba, Grimbergen, Belgium

Juraj Londák Faculty of Electrical Engineering and Information Technology, STU, Bratislava, Slovakia

Said Lotfi Faculty of Science, Laboratory: Natural Resources and Sustainable Development, Ibn Tofail University, Kenitra, Morocco

Jingjing Lou Yiwu Industrial & Commercial College, Yiwu, China

Tasso M. Lugon Innovation Laboratory-LINO, Institute of Information and Communication Technology of Espírito Santo, Vitória, Brazil

Jie Luo China Academy of Telecommunications Technology, Beijing, China

Qingdong Luo Yiwu Industrial & Commercial College, Yiwu, China

Yiyang Luo V.N. Karazin, Kharkiv National University, Kharkiv, Ukraine

V. I. Lutsenko O.Ya. Usikov Institute for Radiophysics and Electronics of the National Academy of Sciences of Ukraine, Kharkiv, Ukraine

Junchao Ma College of Big Data and Internet, Shenzhen Technology University, Shenzhen, China

M. Maccioni Department of Astronautics, Electric and Energy Engineering, Sapienza University of Rome, Rome, Italy

Nikita Magar Pimpri Chinchwad College of Engineering, Pune, India

Sonok Mahapatra Westhill High School, Stamford, CT, USA

Shikha Maheshwari Manipal University, Jaipur, India

Zenzele Malale Department of Computer Science, University of Limpopo, Mankweng, South Africa

Boris Manov South-West University, Blagoevgrad, Bulgaria

Sekgoari Semaka Mapunya Department of Computer Science, University of Limpopo, Mankweng, South Africa

Panagiotis Maroulidis Department of Informatics, Aristotle University of Thessaloniki, Thessaloniki, Greece

Marieta Marres-Salhuana Universidad Autónoma del Perú, Lima, Perú

Hamzah Hadi Masmali School of Electrical Engineering and Computing, The University of Newcastle, Newcastle, NSW, Australia;
College of Business Administration, Jazan University, Jazan, Saudi Arabia

Delvani A. Mateus Innovation Laboratory-LINO, Institute of Information and Communication Technology of Espírito Santo, Vitória, Brazil

Alexander Merkulov Uchi.Ru LLC, Moscow, Russia

Gustavo Mesias Universidad Politécnica Salesiana, Quito, Ecuador;
Universidad Politécnica de Madrid, Madrid, España

Lora Metanova The St. Kliment Ohridski Sofia University, Sofia, Bulgaria

Shah J. Miah Newcastle Business School, University of Newcastle, Callaghan, NSW, Australia

Dariusz Mikulowski Faculty of Exact and Natural Sciences, Siedlce University of Natural Sciences and Humanities, Siedlce, Poland

Valentina Milenkova South-West University, Blagoevgrad, Bulgaria

Mohamed S. Mohamed Department of Computer Engineering, Military Technical College, Cairo, Egypt

Andrey S. Molyakov Institute of IT and Cybersecurity, Russian State University for the Humanities, Moscow, Russia

A. J. Morais Universidade Aberta, Lisboa, Portugal;
LIAAD—INESC TEC, Porto, Portugal

Sorin-Aurel Moraru Transilvania University of Brasov, Brasov, Romania

Davide Moroni National Research Council, Institute of Information Science and Technologies, Pisa, Italy

Kumyszhan Mukasheva Toraigyrov University, Pavlodar, Kazakhstan

Belinda Mutunhu University of South Africa, UNISA, Pretoria, South Africa

Taras Mykytyn Rivne State Humanity University, Rivne, Ukraine

Valentina Narvaez-Teran Cinvestav—Tamaulipas, Victoria Tamps., Mexico

Keerthi Neharika Letterkenny Institute of Technology, Letterkenny, Ireland

Joaquim Neto Universidade Aberta, Lisboa, Portugal;
Laboratório Nacional de Engenharia Civil, Lisboa, Portugal

Ádler O. S. Neves Innovation Laboratory-LINO, Institute of Information and Communication Technology of Espírito Santo, Vitória, Brazil

Alexander Nikolov SYNYO GmbH, Vienna, Austria

Nasimul Noman School of Information and Physical Sciences, University of Newcastle, Callaghan, NSW, Australia

Vincent Omollo Nyangaresi Faculty of Biological & Physical Sciences, Tom Mboya University College, Homabay, Kenya

Mostafa El Ouariachi Laboratory of Electrical Engineering and Maintenance (LEEM), BP: 473 Higher School of Technology, University of Mohammed I, Oujda, Morocco;
Laboratory Renewable Energy, Embedded System and Information Processing, National School of Applied Sciences, University of Mohammed I, Oujda, Morocco

William Oñate Universidad Politécnica Salesiana, Quito, Ecuador;
Universidad Politécnica de Madrid, Madrid, España

Sergey Panfilov Federal Budget-Financed Institution, ”Federal Resources Centre”, Moscow, Russia

M. Paulucci ASM Terni S.P.A, Terni, Italy

Małgorzata Pańkowska University of Economics in Katowice, Katowice, Poland

Dobrinka Peicheva South-West University, Blagoevgrad, Bulgaria

Vlad Ștefan Petre Transilvania University of Brasov, Brasov, Romania

Nikolaos Petrellis Department of Electrical and Computer Engineering, University of Peloponnese, Patras, Greece

Dion Wayne Pieterse California State University, Fullerton, CA, USA

Kornprom Pikulkaew Department of Computer Science and Graduate School, Faculty of Science, Chiang Mai University, Chiang Mai, Thailand

Pavol Podhradský Faculty of Electrical Engineering and Information Technology, STU, Bratislava, Slovakia

P. Poursoltan Department of Astronautics, Electric and Energy Engineering, Sapienza University of Rome, Rome, Italy

Ela Pustulka FHNW University of Applied Arts and Sciences Northwestern Switzerland, School of Business, Institute for Information Systems, Olten, Switzerland

I. Putu Andika Subagya Putra Universitas Pendidikan Ganesha, Singaraja, Bali, Indonesia

Alexander Raikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

Ruwaida Ramly Universiti Kuala Lumpur, Kuala Lumpur, Malaysia

Gabriel Ramírez-Torres Cinvestav—Tamaulipas, Victoria Tamps., Mexico

Vijay Singh Rathor IIS (Deemed to Be) University, Jaipur, India

Sandeep Gogineni Ravindrababu Center for Secure and Dependable Systems, University of Idaho, Moscow, ID, USA

Lilia Raycheva The St. Kliment Ohridski Sofia University, Sofia, Bulgaria

Eduardo Rodriguez-Tello Cinvestav—Tamaulipas, Victoria Tamps., Mexico

Peter Roelofsma Delft University of Technology, Center for Safety in Healthcare, Delft, The Netherlands

Silvia Rus Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany

Dario Russo National Research Council, Institute of Information Science and Technologies, Pisa, Italy

Patrik Rüegg School of Business FHNW, Olten, Switzerland

Wael Saideni XLIM Research Institute, UMR CNRS 7252, Limoges, France

Aznida Abu Bakar Sajak Universiti Kuala Lumpur, Kuala Lumpur, Malaysia

Gouda Salama Department of Computer Engineering, Military Technical College, Cairo, Egypt

Betty Elezebeth Samuel Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia

Christina Samuelsson Department of Biomedical and Clinical Sciences, Linköping University, Linköping, Sweden

Domenico Santaniello DIIN University of Salerno, Fisciano, Italy

Burcu Kir Savaş Kocaeli University Umuttepe Campus, Kocaeli, Turkey

Tatiana Savina Intel Corporation, Nizhny Novgorod, Russia

Carrie Hartley Segal University of California, Santa Barbara, Santa Barbara, CA, USA

Stanislav Selitskiy Earthlink Internet, Atlanta, GA, USA

Padmanayaki Selvarajan Department of Information Technology and Security, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia

Will Serrano The Bartlett, University College London, London, UK

Erika Severeyn Department of Thermodynamics and Transfer Phenomena, Universidad Simón Bolívar, Caracas, Venezuela

Shermin Shamsudheen Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia

Amita Sharma IIS (Deemed To Be University), Jaipur, India

Navneet Sharma Department of CS & IT, IIS (Deemed To Be University), Jaipur, India

Vivek Sharma Department of Computer Science, The Graduate Center, City University of New York, NY, USA

Mykola Shershun Institute of Environmental Management and Agroecology, Ukraine's National Academy of Agrarian Sciences, Kyiv, Ukraine

Guang Shi Nara Institute of Science and Technology, Ikoma, Nara, Japan

Swati Shinde Pimpri Chinchwad College of Engineering, Pune, India

S. M. Shulgar V.N. Karazin, Kharkiv National University, Kharkiv, Ukraine

Ruben Shushardzhan Academy of Rehabilitation Medicine, Clinical Psychology, and Music Therapy LLC, Moscow, Russia

Sergey V. Shushardzhan Academy of Rehabilitation Medicine, Clinical Psychology, and Music Therapy LLC, Moscow, Russia

Xin Su Department of Electronic Engineering, Tsinghua University, Beijing, China

Alexander Suvorov Intel Corporation, Nizhny Novgorod, Russia

Jacek Szklarski Institute of Fundamental Technological Research, Polish Academy of Sciences, Warsaw, Poland

Neha Tiwari IIS (Deemed To Be University), Jaipur, India

Mariyan Tomov The St. Kliment Ohridski Sofia University, Sofia, Bulgaria

Alex Torres University Corporation Comfacauca-Unicomfacauca, Popayán, Colombia

Jan Treur Delft University of Technology, Center for Safety in Healthcare, Delft, The Netherlands;
Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

Naresh Kumar Trivedi Chitkara University Institute of Engineering and Technology, Punjab, India

Alfredo Troiano NetCom Group, Napoli, Italy

Hossana Twinomurinzi University of Johannesburg, Auckland Park, South Africa

Munirul Ula Department of Information System, Universitas Malikussaleh, Aceh, Indonesia

Christoph Uran Research group ROADMAP-5G, Carinthia University of Applied Sciences, Klagenfurt, Austria

Carmine Valentino DIPMAT University of Salerno, Fisciano, Italy

Andriy Valyukh Open International University of Human Development «Ukraine», Rivne, Ukraine

Ad van Berlo Smart Homes, Maarssen, Netherlands

Willeke van Staalduinen AFEdemy, Academy On Age-Friendly Environments in Europe BV, Gouda, Netherlands

Radoslav Vargic Faculty of Electrical Engineering and Information Technology, STU, Bratislava, Slovakia

Mthulisi Velempini Department of Computer Science, University of Limpopo, Mankweng, South Africa

Ricardo Velezmoro-León Universidad Nacional de Piura, Piura, Peru

Neli Velinova The St. Kliment Ohridski Sofia University, Sofia, Bulgaria

Felícita M. Velásquez-Fernández Universidad César Vallejo, Piura, Peru

K. A. Vidhya Department of IST, Anna University, Chennai, India

Anushri Vijay IIS (Deemed To Be University), Jaipur, India

Stefan von Arx FHNW University of Applied Arts and Sciences Northwestern Switzerland, School of Business, Institute for Information Systems, Olten, Switzerland

Xiyuan Wan Yiwu Industrial & Commercial College, Yiwu, China

Xiaodi Wang Western Connecticut State University, Danbury, CT, USA

Tyler Wooldridge Western Connecticut State University, Danbury, CT, USA

Helmut Wöllik Research group ROADMAP-5G, Carinthia University of Applied Sciences, Klagenfurt, Austria

Limin Xiao Department of Electronic Engineering, Tsinghua University, Beijing, China

Alina Yakymchuk National University of Water and Environmental Engineering, Rivne, Ukraine

Kyoungil Yoon Graduate School, Dept. of Information Science, Korea National Open University, Seoul, Korea

Ling Yu Inspur Academy of Science and Technology, Jinan, Shandong, China

Fahim Yusuf Daffodil International University, Dhaka, Bangladesh

Zahura Zaman Daffodil International University, Dhaka, Bangladesh

Ela Zawidzka Institute of Fundamental Technological Research, Polish Academy of Sciences, Warsaw, Poland

Machi Zawidzki Institute of Fundamental Technological Research, Polish Academy of Sciences, Warsaw, Poland

Jie Zeng Department of Electronic Engineering, Tsinghua University, Beijing, China

Zakaria Zgourdah Faculty of Science, Laboratory: Natural Resources and Sustainable Development, Ibn Tofail University, Kenitra, Morocco

Hui Zhang Inspur Academy of Science and Technology, Jinan, Shandong, China

Renyuan Zhang Nara Institute of Science and Technology, Ikoma, Nara, Japan

Jing Zhao Shandong Yingxin Computer Technology Co., Ltd., Jinan, China

Pengfei Zheng Yiwu Industrial & Commercial College, Yiwu, China;
East China University of Science and Technology, Shanghai, China

Engelika Zhumataeva Toraigyrov University, Pavlodar, Kazakhstan

Mohd Hanif Zulfakar Universiti Kebangsaan Malaysia, Bangi, Malaysia

Visualizing Student Engagement and Performance in Online Course: A Step to Smart Learning Environment

Iman Al-Kindi and Zuhoor Al-Khanjari

Abstract Students' Engagement and Performance (EP) of online courses are analyzed and visualized in order to assist instructors in improving student's performance at an early stage before the end of the academic semester. A fully online course for undergraduate students in the Department of Information Studies, College of Education, Sultan Qaboos University (SQU), was conducted. The total number of students in the course was 38. Students studied each course module and the instructor evaluated them based on a set of assessments. This paper explores the existence of possible relationships between student's engagement and performance. In this paper, the authors only considered the results of the Mid Term Exam part. They extracted the necessary data for analysis purposes for the above-mentioned factors from the log file of the course. The results revealed promising relationships between the student's engagement and performance. This indicates the importance of conducting this kind of case study as a step forward to achieve a smart learning environment.

Keywords Smart learning environment · Student's engagement · Student's performance · Moodle · Log file · Online courses

1 Introduction

Smart Learning Environment (SLE) needs to be enriched in order to advance the educational environment with regards to computers, networks, content, student, instructors, etc. [1]. A smart learning environment may contain features for struggling students (instructors identify and support problematic students), motivation, and efficiency in order to increase engagement, effectiveness, and efficiency (instructors take

I. Al-Kindi (✉) · Z. Al-Khanjari
Department of Computer Science, College of Science, Sultan Qaboos University, Muscut, Sultanate of Oman
e-mail: m109107@student.squ.edu.om

Z. Al-Khanjari
e-mail: zuhoor@squ.edu.om

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_1

the time and make efforts to gain attention, provide feedback to improve student confidence and satisfaction) [2]. On a wide sustainable scale, the smartness of learning environments was defined by their engagement, efficacy, and efficiency. Increased technological innovation has led to various changes in student behavior as well as the modeling of instructional approaches [3]. The learning environment needs to be efficient and provides more productive learning management as a way to enhance smart learning [4]. There is no question that students are important participants in all learning processes.

The National Student's Engagement Survey describes five clusters of student's engagement activities, including the level of academic difficulty, a supportive campus atmosphere, enriching educational interactions, the interaction between students and instructors, and active and collaborative learning [5]. SLE should log every single detail of the behavior of students. It also offers an exceptional opportunity for different stakeholders, such as higher educational institutions, students, instructors, and researchers, to access valuable knowledge by evaluating these behaviors [6]. Furthermore, knowing the basic criteria of students with various personality characteristics will help instructors identify acceptable teaching methods when teaching online courses [7]. The performance of students has been an area of concern for higher education institutions. The study of factors related to the performance of university students has become a subject of increasing interest in the higher education community [8].

The present study thus set out to examine to explore the possible relationship between student's engagement and performance by taking one component from the online course, which is "Mid Term Exam" and analyzing the data of the log file of this component to check this relationship. The paper is organized as follows: Sect. 2 briefly provides a literature review of the importance of student's engagement and performance. Section 3 presents the method by the authors to prove the concept of this study. Section 4 presents the results and discussion. Finally, Sect. 5 concludes the paper.

2 Literature Review

Most of the existing literature pay special attention to the student's attributes: student's engagement and student's performance. Some of the studies discuss one attribute and others examined two attributes. This is shown in Table 1.

Table 1 Literature review studies

Author/year	Purpose of study/focus on
[9]/2021	The authors analyzed the trends of behavioral engagement of 306 undergraduate students taking a degree course partly taught at university online. The authors discovered that students' degrees of involvement had a statistically significant impact on their learning outcomes
[10]/2020	The authors examined the connection between the level of engagement of students in technology-enhanced learning (TEL) and student's performance. The analysis indicated that high-performance learners found it easier to focus than average and low performers when interacting with learning technology
[11]/2019	Understanding how to promote interactive knowledge creation processes is important for the evolution of online learning environments and build learning environments that foster positive participation and interactions between students. The authors looked at the various methods of awareness development in preservice teacher education by looking at students' cognitive engagement and performance in online discussion groups. Multiple regression analysis revealed that different levels of cognitive presence were associated with student performance
[12]/2018	Based on the context, the authors examined how student's behavioral engagement has evolved and illustrated the need for a finer scale of engagement. They observed that behavioral engagement and student's interaction with peers were not a standardized correlation, but there was an interaction between students and the instructor and thus was indicative of increased engagement
[13]/2018	Based on Moore's interaction theory, the authors investigated student perceptions of various engagement techniques employed in online courses. Their study looked at how students understand engagement strategies based on their age, ethnicity, and years of the online learning experience. The findings showed implications for teachers who are interested in the study
[14]/2017	The authors examined E-Learning connection indicators and created a model to clean and delve into the educational specifics in order to construct the student's profile. The E-Learning framework will be able to fully meet and lead the learning behavior of students, provide a personalized learning environment, and promote E-Learning optimization thanks to the user profile analysis

3 Method

3.1 Context and Sample

One of the LMS platforms that are used in the learning and teaching process by integrated courses along with face-to-face teaching is the Modular Object-Oriented Developmental Learning Environment (Moodle). SQU uses Moodle LMS in teaching besides traditional learning. In other words, SQU is using blended learning [15]. A fully online course, "Search Strategies on the Internet" was used as a case study in this paper, which was given in fall 2019. The total number of students enrolled in it was 38. The course aims to provide university students with specialized skills in how to search for various information sources, including websites, search engines, objective evidence, library indexes, and databases, and to be familiar with the various digital information sources available electronically. The course was taught in the Arabic language consisted of different modules distributed over 15 weeks for one academic semester, between recorded electronic lectures, in addition to some live lessons, exams (Mid Term and Final Exam), visual video presentations, assignments, as well as weekly discussions through the forums accompanying each of the course topics. Al-Kindi et al. [16] propose a new model, which is supposed to help in tracking the student's activities in one of the selected courses. The proposed test model goes through a specific process starting from student's engagement, then student's behavior, followed by the student's personality and ending with checking the student's performance. At last, the outcomes obtained from the predictive model of the EBP should boost and enhance the performance of students in the online course [17].

3.2 Data Analysis

To determine the hypothetical relationship between student's engagement and performance, an analysis of course log file extracted from Moodle has been used. The authors then analyzed the data based on the below measurements:

- **Performance**: Mid Exam component (20 marks).
- **Engagement**: The total number of activities undertaken by each student for Mid Exam component only.

4 Interpreting the Results

4.1 Preparing Performance and Engagement Factors Extracting Performance Value

The performance factor is calculated based on the mark of the Mid Exam. The full mark is 20. So, the student ID of the student and his/ her mark of Mid Exam are preserved. The other details are removed. The value is transformed to range 100 by multiplying the value by 5 (20 * 5 = 100). The data is shown in Table 2. It is clear that the performance values of students are in the same close range.

The percentiles method was used to divide the numerical data into groups in this study. A percentile is a statistic that provides the relative location of a numerical data point in distribution as opposed to all other data points [18]. It works by splitting the data into uneven intervals, each of which corresponds to a distinct category. By splitting the time, students' marks are divided into three categories (High, Average and Low), as follow [19]:

- Low: 0.00–35

Table 2 Values of student's performance factor (*the data available on request)

Student ID	Performance 20	Transformed performance 100
1000	16.5	82.5
1001	15.25	76.3
1002	17	85.0
1003	18	90.0
1004	13.5	67.5
1005	15.75	78.8
1006	14.75	73.8
1007	17.25	86.3
1008	16	80.0
1009	16.25	81.3
1010	13	65.0
…	…	…

Table 3 Categories of student's performance factor (*the data available on request)

Student ID	Performance	Category performance
1000	82.5	High
1001	76.3	High
1002	85.0	High
1003	90.0	High
1004	67.5	Average
1005	78.8	High
1006	73.8	Average
1007	86.3	High
1008	80.0	High
1009	81.3	High
1010	65.0	Average
…	…	…

- Average: 35.1–75
- High: 75.1–100.0

The marks of students using categories are shown in Table 3.

4.2 Extracting Engagement Value

The number of actions in the log file of Mid Exam, which are conducted by him/her, represents the engagement of a student. This means, in the file "Mid Exam," the actions for each student in the column "Event name" was counted. These values are converted to be in the range of 100 by multiplying the value by 1.6667 as the maximum value is 60. Table 4 illustrates the engagement for each student and the transformed value.

Same to performance factor, these values are represented by three categories (High, Average, Low) by dividing the period as follow:

- Low: 0.00–35
- Average: 35.1–75
- High: 75.1–100.0.

Table 5 shows the Engagement factor with transformed values and categories.

Table 4 Values of student's engagement factor (*the data available on request)

Student ID	Engagement	Transformed engagement
1000	19	31.7
1001	28	46.7
1002	19	31.7
1003	27	45.0
1004	34	56.7
1005	26	43.3
1006	27	45.0
1007	18	30.0
1008	22	36.7
1009	30	50.0
1010	29	48.3
…	…	…

Table 5 Categories of student's engagement factor (*the data available on request)

Student ID	Transformed engagement	Category
1000	31.7	Low
1001	46.7	Average
1002	31.7	Low
1003	45.0	Average
1004	56.7	Average
1005	43.3	Average
1006	45.0	Average
1007	30.0	Low
1008	36.7	Average
1009	50.0	Average
1010	48.3	Average
…	…	…

4.3 The Relationship Between Student's Engagement and Student's Performance

The details of two factors categories for the 38 students are illustrate in Table 6.

The entire distribution of data regarding student engagement and performance is depicted in Fig. 1. Some of the students' performance is impacted by their engagement, as evidenced by following up the specifics of students and observation of Fig. 1, as, mostly when the factor of engagement is "High" and "Average" the factor of performance can be "High." On the other hand, when the engagement factor is "Low" the performance will be "Low" as with "student ID: 1026."

4.4 Extracted Rules

Based on Table 6, the summary of relationships between the two factors as follows in Table 7, where the shortcut represents:

- HE: High Engagement
- HP: High Performance
- AE: Average Engagement
- AP: Average Performance
- LE: Low Engagement
- LP: Low Performance.

And the numbers represent the number of cases among the students.

Based on Table 7, the summary of relationships between the factors is converted into a group of condition rules (If–then) [19]. These rules are true for most cases in the dataset, but it does not reflect the relationship between all factors. The rules are:

- If (Engagement = High)
- Then Performance = High
- If (Engagement = High)
- Then Performance = Average
- If (Engagement = Average)
- Then Performance = High
- If (Engagement = Average)
- Then Performance = Average
- If (Engagement = Low)
- Then Performance = High
- If (Engagement = Low)
- Then Performance = Low.

Table 6 The details of the engagement factor and performance factor with categories

Student ID	Engagement	Performance
1000	Low	High
1001	Average	High
1002	Low	High
1003	Average	High
1004	Average	Average
1005	Average	High
1006	Average	Average
1007	Low	High
1008	Average	High
1009	Average	High
1010	Average	Average
1011	Average	High
1012	Average	Average
1013	Low	High
1014	Average	High
1015	Average	Average
1016	Average	High
1017	Low	High
1018	High	Average
1019	Average	High
1020	Average	High
1021	Average	High
1022	Average	Average
1023	High	High
1024	Low	High
1025	Average	High
1026	Low	Low
1027	Average	High
1028	Average	High
1029	High	High
1030	Average	Average
1031	Average	High
1032	Average	High
1033	High	Average
1034	Average	Average
1035	Low	High
1036	Average	Average
1037	Average	Average

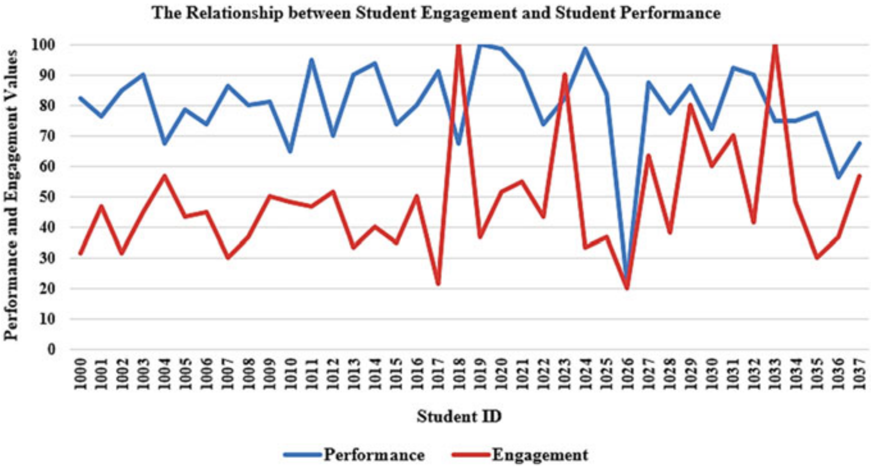


Fig. 1 Relationship between student's engagement and student's performance

Table 7 Summary of relationships between student's engagement and student's performance

Engagement and performance	LE	AE	HE
LP	1	0	0
AP	0	10	2
HP	7	16	2

5 Conclusion

The results of analyzing the data of this course for the Mid Term exam component only prove that there is a relationship between engagement and performance of the student. The analysis shows that when the factor of engagement is "High" and "Average" among the dataset, which is 38 students, the category of performance appears to be "High." On the other hand, in ten cases, the categories of engagement and performance were matching "Average." One of the drawbacks of this study is that, limiting the experimenting on one course as a case study due to time constraints.

In the future, the authors will extend the analysis to investigate again the possible relationship between the two factors to consist of more components of the course not only one. Also, doing more experimentation on more courses. In addition, developing a support tool for instructors to assist them in predicting student's performance during the early phases of the academic semester.

More in more, the enhancement of educational teaching strategies is required in terms of giving more attention to student's engagement such as but not limited to the activities students engaged in the courses and the interaction with the instructor to foster student's performance during fully online courses. The authors recommend, future researchers focus on analyzing the log file of student's courses to better understand their engagement and performance in online courses. This will lead to making their learning environment more efficient and sustainable.

Acknowledgements The authors would like to express their gratitude to Sultan Qaboos University's College of Science and Computer Science. Prof. Zuhoor Al-Khanjari is supervising this project, which is funded by a Doctoral Program scholarship from Sultan Qaboos University.

References

1. Al-Kindi I, Al-Khanjari Z (2019) The smart learning management system (SLMS). In: Free and open-source software conference (FOSSC-2019), February 8–9, Sultanate of Oman (Muscat). ISSN: 1813–419X (2019). https://fossc.om/2019/wp-content/uploads/2019/03/Proceedings.pdf#page=32
2. Spector J (2017) Conceptualizing the emerging field of smart learning environments. Smart Learn Environ 1(1):2. https://doi.org/10.1186/s40561-014-0002-7
3. Nikolov R, Shoikova E, Krumova M, Kovatcheva E, Dimitrov V, Shikalanov A (2016) Learning in a smart city environment. J Commun Comput 13:338–350 (2016). https://doi.org/10.17265/1548-7709/2016.07.003
4. Nakayama M, Mutsuura K, Yamamoto H (2014) Impact of learner's characteristics and learning behaviour on learning performance during a fully online course. Electron J e-Learn 12(4):394–408 (2014). https://www.academic-publishing.org/index.php/ejel/article/view/1708/1671
5. Young M, Robinson S, Alberts P (2009) Students pay attention! Combating the vigilance decrement to improve learning during lectures. Act Learn High Educ 10(1):41–55. https://doi.org/10.1177/1469787408100194
6. Yassine S, Kadry S, Sicilia M (2016) Measuring learning outcomes effectively in smart learning environments. In: 2016 smart solutions for future cities, February 7–9, Kuwait. IEEE, pp 1–5. https://doi.org/10.1109/SSFC.2016.7447877
7. Bhagat K, Wu L, Chang C (2019) The impact of personality on students' perceptions towards online learning. Austral J Educ Technol 35(4) (2019). https://doi.org/10.14742/ajet.4162
8. Shahzadi E, Ahmad Z (2011) A study on academic performance of university students. In: Eighth international conference on recent advances in statistics "statistics, biostatistics and econometrics, February 8–9, Lahore, Pakistan, pp 255–268. http://www.isoss.net/downloads/proc%208th%20.pdf#page=268
9. Chen C, Meng X (2021) Exploring the relationship between student behavioral patterns and learning outcomes in a SPOC. Int J Distance Educ Technol (IJDET) 19(1):35–49. https://doi.org/10.4018/IJDET.2021010103
10. Bergdahl N, Nouri J, Fors U, Knutsson O (2020) Engagement, disengagement and performance when learning with technologies in upper secondary school. Comput Educ 149:103783. https://doi.org/10.1016/j.compedu.2019.103783
11. Galikyan I, Admiraal W (2019) Students' engagement in asynchronous online discussion: the relationship between cognitive presence, learner prominence, and academic performance. Internet Higher Educ 43:100692. https://doi.org/10.1016/j.iheduc.2019.100692
12. Nguyen T, Cannata M, Miller J (2018) Understanding student behavioral engagement: importance of student interaction with peers and teachers. J Educ Res 111(2):163–174. https://doi.org/10.1080/00220671.2016.1220359
13. Martin F, Bolliger D (2018) Engagement matters: student perceptions on the importance of engagement strategies in the online learning environment. Online Learn 22(1):205–222. https://doi.org/10.24059/olj.v22i1.1092

14. Liang K, Zhang Y, He Y, Zhou Y, Tan W, Li X (2017) Online behavior analysis-based student profile for intelligent E-learning. J Electr Comput Eng. https://doi.org/10.1155/2017/9720396
15. Al-Kindi I, Al-Khanjari Z (2020) A novel architecture of SQU SMART LMS: the new horizon for SMART City in Oman. In: 2020 third international conference on smart systems and inventive technology (ICSSIT). IEEE, pp 751–756. https://doi.org/10.1109/ICSSIT48917.2020.9214141
16. Al-Kindi I, Al-Khanjari Z, Al-Salmi J (2020) Managing the triangular bond of the EBP for SQU students through the proposed test model. Int J Eng Adv Technol (IJEAT) 1(1):391–400. ISSN 2249-8958. https://doi.org/10.35940/ijeat.A1914.1010120
17. Al-Khanjari Z, Al-Kindi I (2020) Proposing the ebp smart predictive model towards smart learning environment. J Talent Dev Excell 12(2s):2422–2438. https://iratde.com/index.php/jtde/article/view/959
18. Lavrakas P (2008) Percentile. Encyclopedia of survey research methods. https://doi.org/10.4135/9781412963947.n373. Retrieved from: https://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n373.xml. Last accessed: 10 Jan 2021
19. Al-Kindi I, Al-Khanjari Z (2021) Exploring factors and indicators for measuring students' performance in moodle learning environment. Int J Emerg Technol Learn 16(12). https://doi.org/10.3991/ijet.v16i12.22049

IoT Automated Pill Dispenser for Elderly Care

Saidatunnajwa Abdul Aziz, Aznida Abu Bakar Sajak, Ruwaida Ramly, and Mohd Hanif Zulfakar

Abstract This project is fabricated to ease medication consumption, especially for the elderly that always forget the proper time to consume their prescribed medicine. Thousands of cases have been recorded throughout the decade of wrong consumption of medicine. This may lead to serious issue as improper medicine dose is ineffective for the sickness that they suffer. This paper aims to develop an automated pill dispenser that triggers the alarm to the elderly, records the medication drop data using ThingSpeak, and notifies the caretaker through the Blynk application. This paper uses Arduino ATmega 2560 as the microcontroller for the device. It will be connected to a Wi-Fi module to transmit the data for the ThingSpeak platform and notifies the caretaker through the Blynk application. The paper will surely help eliminate the underdose and overdose issue, especially among the elderly and ease guardian's worries about their absentness at the moment of medicine consumption. It is hoped that this paper can be used to replace hand-held pillbox device that is a hassle toward the elderly.

Keywords Smart health care · Internet of Things · Arduino · Pill dispenser · Easy medication · Wi-Fi

1 Introduction

Chronic disease among the elderly is a common issue these days. Most elderly suffer from at least one chronic condition that requires lifelong medical supplies. This may lead them to consumed medication each day accordingly to prescription by the doctors. As they are growing older, the elderly might also suffer from Alzheimer's, also known as a disease that slowly erases the memories of the elderly. They end up needing help from caretaker and guardian. This paper aims to help specifically

S. A. Aziz · A. A. B. Sajak (✉) · R. Ramly
Universiti Kuala Lumpur, 50250 Kuala Lumpur, Malaysia
e-mail: aznida@unikl.edu.my

M. H. Zulfakar
Universiti Kebangsaan Malaysia, 50300 Bangi, Malaysia

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_2

the elderly to eat their pills on time despite the absence of a caretaker. The caretaker can refill the prescribed medications weekly, and after six hours, the pill will automatically dispense. An alert and frequency data could be monitored through Blynk and ThingSpeak, respectively, as in [1, 4, 5, 8, 12, 13] via Wi-Fi as the transmission medium. A study stated that 40% up to 75% of elderly fails to consume their medication properly despite the provided clear prescription details [9]. Some elderly forget that they have taken their pills, thus consuming them repeatedly, resulting in overdoses cases. Both underdose and overdose cases are dangerous, as both may lead to severe consequences for the elderly. The elderly should adhere to the prescription schedule, and constant help from the caretaker is needed if the elderly cannot take medicine regularly.

Several existed papers have pursued the same aims as the proposed papers, which is to develop a device that automatically dispenses medications for the elderly. However, all these papers do not state their refillable basis, and most of them do not analyze the data taken from the frequency of medication. This is the contribution of this paper. The data stored in the cloud via ThingSpeak can be used for the patient's medication history or any medical needs in the future. The current technology [1, 4, 5, 8, 12, 13] does not implement the Internet of Things (IoT) in their device as the device could not be managed through any mobile applications. These IoT features are beneficial in terms of their ability to control the device through applications. This paper will be useful in eliminating any chances of overdose and underdose medication specifically toward the elderly and helps the caretaker ensure that the elderly consumed their medicines on time.

2 Research Methodology

The interactive waterfall model [11] is the methodology that will be used throughout this paper. Its adaptable and simple features are essential in making sure the project in this paper working well accordingly to its timeline. The main factor of choosing this model is its ability to change according to the current situation in each phase, such as redesigning any changes if required. Figure 1 shows the stages of the model and an explanation of each phase. Each phase shows a specific different process that is reviewable.

2.1 Feasibility Study

A feasibility study is the first phase in fabricating this paper. This phase aims to evaluate the importance of this device, especially toward the elderly and the elderly's guardian. Once the topic is discerned, the paper's proposal is written, which features the objectives and the paper's scope. This phase started by recognizing the increasing trend of the elderly's mismanage of medicine consumption and highlighting ways to

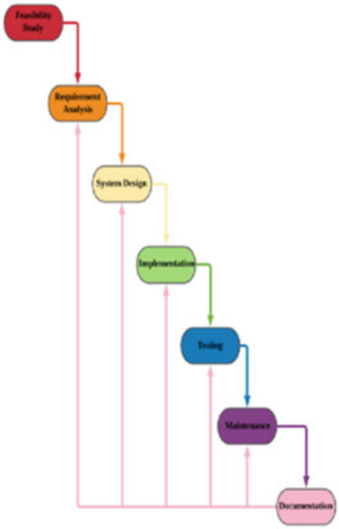


Fig. 1 Iterative waterfall model

ease the guardian job in making sure the elderly consumed their medicine on time despite the guardian's absentness.

2.2 *Requirement Analysis*

The requirement analysis of software and hardware needed is listed to develop the proposed paper through this phase. The information on the proposed paper was gathered through research and literature review of the existing paper that features similar objectives with the proposed paper. Both possible hardware and software components required by the proposed paper were decided through this phase too. The block diagram is shown in Fig. 2.

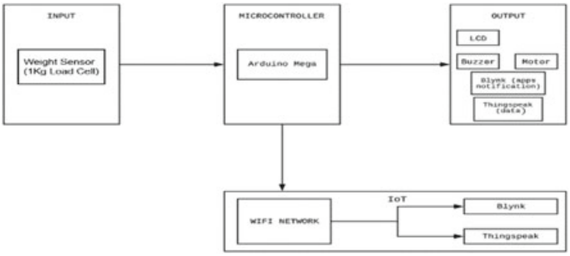


Fig. 2 Block diagram

2.3 System Design

The system design phase is a phase that the developers illustrate the concept of the proposed paper using the information gathered from the previous phase. This paper is proposed to ensure proper medication consumption for the elderly who have difficulties remembering their medication schedule. The Arduino [10] will attach with the other hardware that offers different functions. Once the buzzer ring, a notification will be sent to the Blynk as the alert system for the caretaker. The medication drop data will then be recorded for further data analysis by the doctors using ThingSpeak. The flowchart of the project is shown in Fig. 3.

2.4 Implementation Phase

In this phase, the developers need to start implementing each separate component into one device. Then, the developers can start building the device by following the design created in the previous phase. The developers will fabricate the device and compile the coding needed for the software and controller.

2.5 Testing Phase

This phase is crucial in making sure that no unexpected error occurs in future. Any error and problem should be solved, and the detail can be recorded for future use. As for the hardware testing, each component is tested individually, and once the device is put together, it will be tested again. The software used by the developer will go under certain testing to ensure the operability of the device. In software testing, the developer needs to make sure that the software can perform according to the requirements stated and compile the coding without showing any error. Both the device and software connectivity will be checked too. The final testing is equally important as it is to assure excellent connectivity of the device and software. Section 4 discusses more on this phase.

2.6 Maintenance Phase

During the maintenance phase, the troubleshooting will be done to the paper if any error occurs while running the program. This troubleshooting will not be done regularly and only run when needed. After the troubleshooting is done, the developer can proceed to the next phase, the documentation phase.

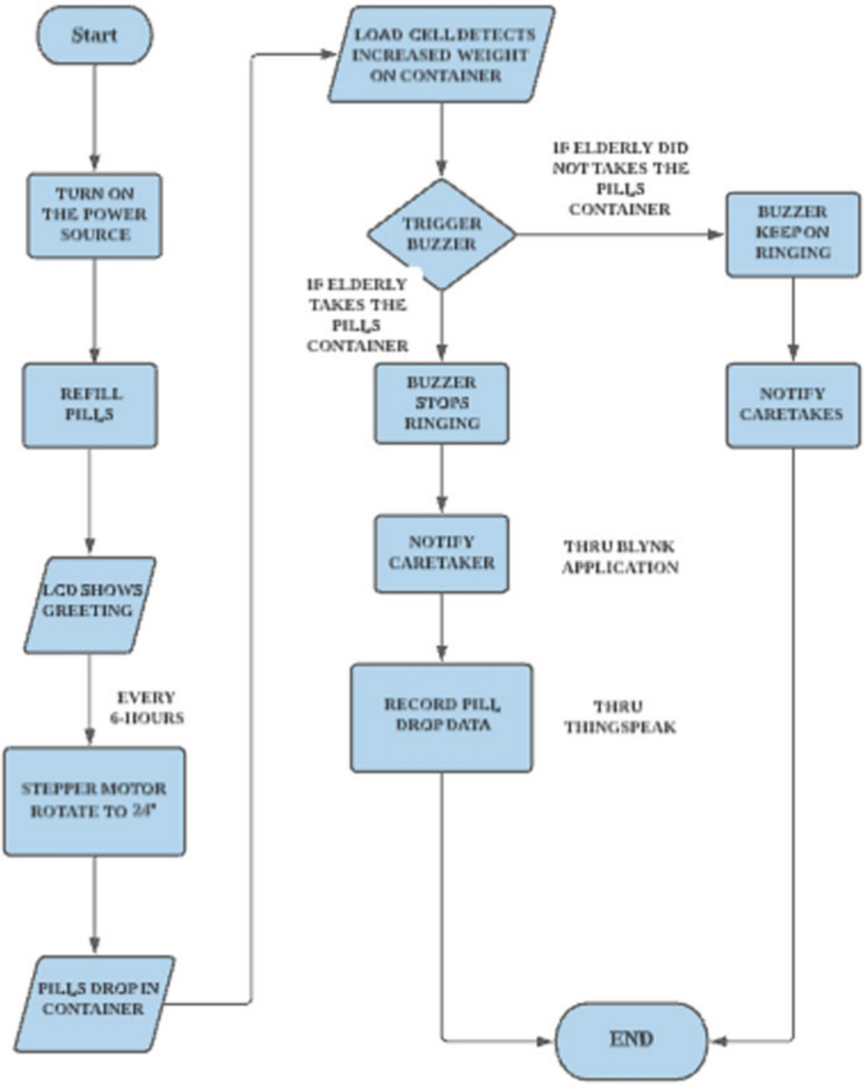


Fig. 3 Flowchart

2.7 Documentation Phase

Documentation is the last phase for the iterative waterfall model methodology method. All the previous phases are documented in a paper report so that the evaluation could be done for the whole progress of this paper. This paper is the outcome of this process.

3 Hardware and Software

3.1 Hardware Development

Two parts of hardware are featured in this paper. The first part is the pill dispenser that rotates every six hours using a stepper motor, and the second part is the load cell that detects the weight changes and triggers the buzzer once the pill drops into the container (Table 1).

Pill Dispenser This dispenser is made with the design of 15 compartments. One compartment is spared as the pill drop segment, and it is hollowed out. The other 14 segmentation is used to store the pills. The container is not connected, and the elderly could pick up the container to consume their medications (Fig. 4).

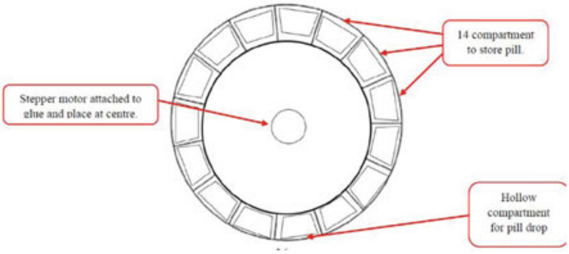
This dispenser is rotated using a stepper motor. The stepper motor will rotate to each compartment at 24° per angle. The time interval for the stepper motor to rotate is set in the coding. The caretaker will refill the medication into each compartment weekly (Fig. 5).

Stepper Motor The stepper motor is used in this paper as this motor rotates at a specified angle. The angle is set to 24° for each compartment with 14.29 steps for each revolution. In this paper, the stepper motor used X113647 as its driver module. It is connected to Arduino Mega through pin as below.

Table 1 List of hardware and software

	Item	Unit
Hardware	Pill dispenser	1
	Stepper motor	1
	Buzzer	1
	Load cell	1
	LCD	1
Software	Arduino IDE	–
	Blynk	–
	ThingSpeak	–

Fig. 4 Pill case design


14 compartment to store pill.
Stepper motor attached to glue and place at centre.
Hollow compartment for pill drop

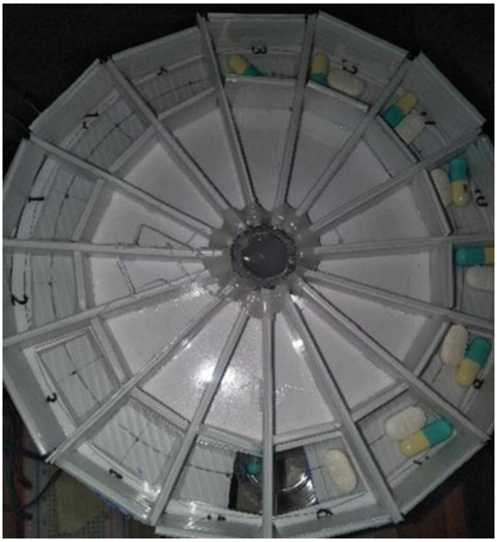


Fig. 5 Real-life pill dispenser

Piezo Buzzer In this paper, the piezo buzzer is used to trigger the alarm to the elderly as an alert for the medication time. Piezo buzzer can generate up to 1150 dB. It is connected to pin 10 in the Arduino microcontroller.

Load Cell A load cell [6] is a device that converts weight sensor quantity into electrical output. This device [7] is used to weigh objects, and it is made to amplify the signals from the load cell then reports to the microcontroller. The weight sensor is first connected to its HX711 module according to the specified pin (Fig. 6).

Liquid Crystal Display (LCD) The liquid crystal display displays the greeting as the power is connected and when the pill drops (Figs. 7 and 8).

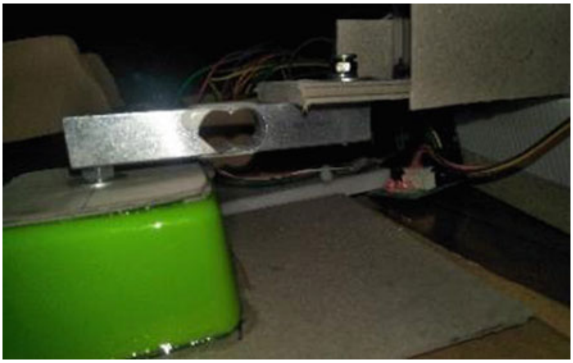


Fig. 6 Load cell

Fig. 7 LCD for greetings

Fig. 8 LCD when pill drop

Table 2 Pin description

VDD	+5 V Pin
VSS	GND
RS, EN, V0	Pin 12, 11, potentiometer
D4, D5, D6, D7	Pin 16, 17, 18, 19

The LCD is connected to Arduino Mega for connectivity. The potentiometer is used to control the brightness of the display. The pins are assigned as followed, respectively (Table 2).

Complete Prototype The complete prototype of the automated pill dispenser for the elderly will be displayed in this section. The first part is the dispenser rotated every six hours using a stepper motor, and the second part is the load cell that detects the weight changes and triggers the buzzer once the pill drops into the container (Figs. 9 and 10).

All hardware components are configured through Arduino using C++ language. Once the pill drops into the container, the 1 kg load cell will detect weight changes and send the information to the buzzer to trigger the alarm for the elderly. If the pill remains to be in the container, the buzzer will keep on ringing. The notification will also be sent into the caretaker’s Blynk application repeatedly if the elderly still did not pick up the container from the holder. At the same time, the medical drop data will be stored in the ThingSpeak to allow further analysis by the doctors. Once the container is picked up from the holder, the buzzer will stop ringing, and the notification will stop looping. The elderly need to put the container back into the holder for the next medication time.

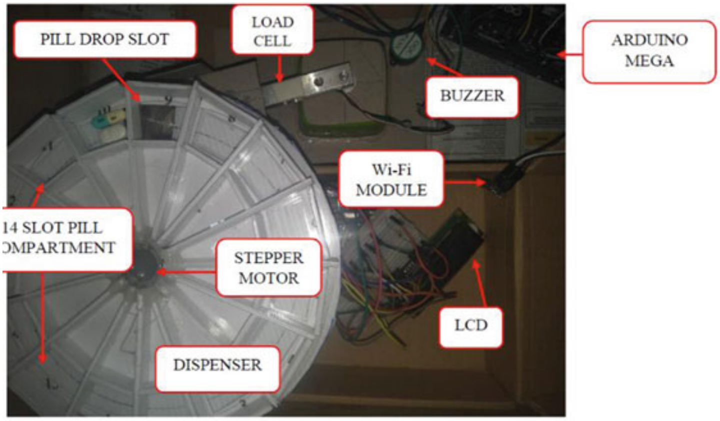


Fig. 9 Complete prototype part one

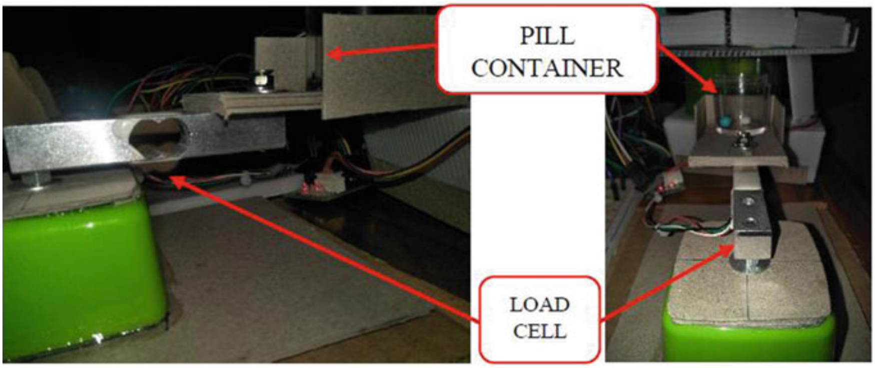


Fig. 10 Complete prototype part two

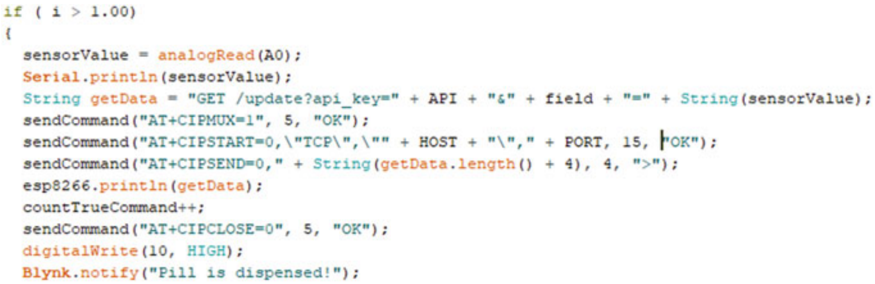
3.2 *Software Development*

This section will explain the complete programming code of automated pill dispenser for elder for each hardware and software featured.

Stepper Motor Programming Code This code is used to rotate the dispenser every six hours-time intervals for medication drop. In this code, the six hours-time intervals and the stepper motor angle movement are set.

LCD Programming Code This code is used to display the greeting and time for pill alert on LCD.

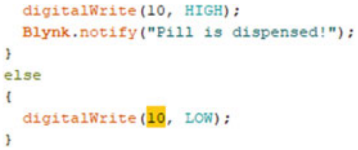
Load Cell Programming Code This code is used to calibrate load cell according to their range of weight detection. Once the load cell finishes calibrating, set up the code for the load cell to detect the pill's increasing weight (Fig. 11).



```
if ( i > 1.00)
{
  sensorValue = analogRead(A0);
  Serial.println(sensorValue);
  String getData = "GET /update?api_key=" + API + "&" + field + "=" + String(sensorValue);
  sendCommand("AT+CIPMUX=1", 5, "OK");
  sendCommand("AT+CIPSTART=0,\"TCP\",\"" + HOST + "\"," + PORT, 15, "OK");
  sendCommand("AT+CIPSEND=0," + String(getData.length() + 4), 4, ">");
  esp8266.println(getData);
  countTrueCommand++;
  sendCommand("AT+CIPCLOSE=0", 5, "OK");
  digitalWrite(10, HIGH);
  Blynk.notify("Pill is dispensed!");
```

Fig. 11 Load cell setup code

Fig. 12 Buzzer alert coding



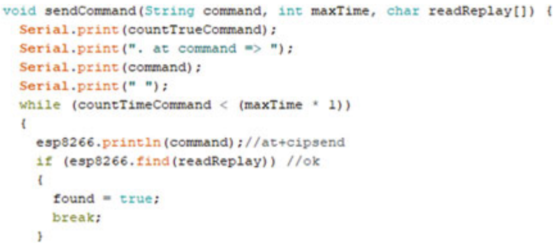
```
  digitalWrite(10, HIGH);
  Blynk.notify("Pill is dispensed!");
}
else
{
  digitalWrite(10, LOW);
}
```

Buzzer Alert Programming Code This code is included in the load cell coding to trigger only when the load cell detects increasing weight (Fig. 12).

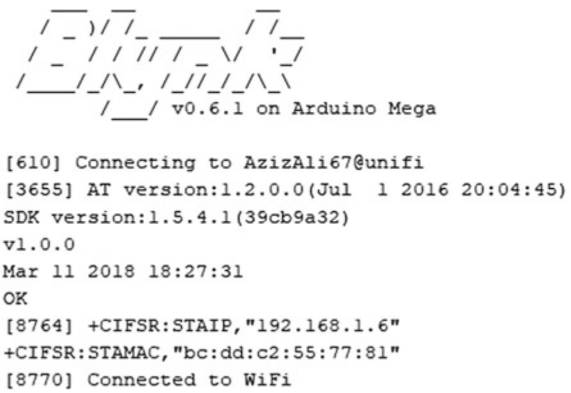
ThingSpeak Programming Code First, we need to create the ThingSpeak account and copy the API key. Then, paste the API key in the ThingSpeak coding in Arduino IDE to ensure the working connection with the hardware. Then, set up the configuring code for the connection to store the medication drop data in ThingSpeak (Fig. 13).

Blynk Programming Code First, copy the authentication token sent to the developer email from the Blynk app. Then, paste the authentication token into the configuration code in Arduino IDE. Then, set up the code for Blynk configuration in Arduino IDE. Include Blynk command into load cell setup code to ensure that it only notifies the caretaker when the pill drops into the container. Next, loop the notification on the Blynk app by including the Blynk.run into the loop() coding. Then, include the code to start the Blynk app notification (Fig. 14).

Fig. 13 Configuring code for ThingSpeak



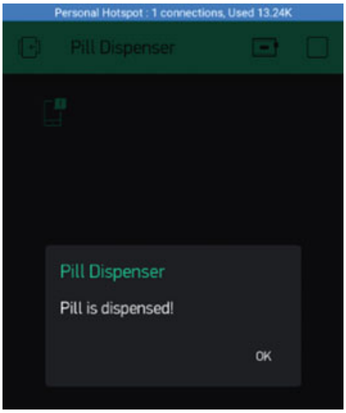
```
void sendCommand(String command, int maxTime, char readReplay[]) {
  Serial.print(countTrueCommand);
  Serial.print(". at command => ");
  Serial.print(command);
  Serial.print(" ");
  while (countTimeCommand < (maxTime * 1))
  {
    esp8266.println(command);//at+cipsend
    if (esp8266.find(readReplay)) //ok
    {
      found = true;
      break;
    }
```



```
    ___  __          __
   / _ )/ /_ _____  / /__
  / _  / / // / _ \/  '_/
 /____/_/\_, /_//_/_/\_\
        /___/ v0.6.1 on Arduino Mega

[610] Connecting to AzizAli67@unifi
[3655] AT version:1.2.0.0(Jul  1 2016 20:04:45)
SDK version:1.5.4.1(39cb9a32)
v1.0.0
Mar 11 2018 18:27:31
OK
[8764] +CIFSR:STAIP,"192.168.1.6"
+CIFSR:STAMAC,"bc:dd:c2:55:77:81"
[8770] Connected to WiFi
```

Fig. 14 Blynk has been successfully connected



Pill is dispensed!

Fig. 15 Blynk is connected, and the notification pop up indicates the medication time

Blynk Notification for the Caretaker This notification will pop up on the caretaker's smartphone when the pill drops into the dispenser to monitor the medication time even when they are away from the elderly (Fig. 15).

4 User Testing and Discussion

4.1 User Testing

Dispenser rotates then pill(s) are dispensed The dispenser will remain idle until the six hours-time interval approach, and then, it will rotate to 24° for the pills to drop into the hollowed compartment (Figs. 16 and 17).

Buzzer triggers alarm to alert the elderly Besides that the buzzer will trigger the alarm continues to alert the elderly (Fig. 18).

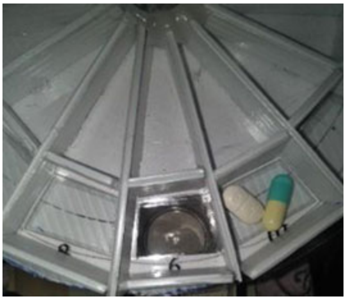


Fig. 16 Dispenser in idle position

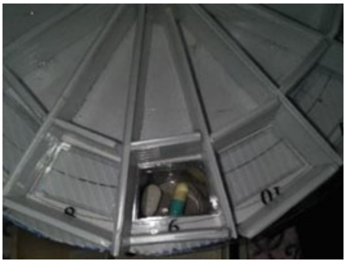


Fig. 17 Dispenser rotated and pill drops

Fig. 18 Buzzer triggers alarm for elderly

LCD light up as an alert Then, the LCD will light up as the alert simultaneously (Fig. 19).

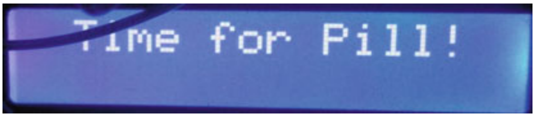
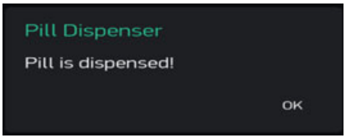


Fig. 19 LCD light up with the alert



Pill Dispenser

Pill is dispensed!

Fig. 20 Blynk notification

Blynk Notification Blynk application [3] will notify the caretaker of the medication dispensed. The alerts and notification would be in the loop if the elderly did not take the medication container out of its holder (Fig. 20).

Alert and notification stop Once the pill container is taken out, all of the alerts will stop, and it is ready for the next medication time. The elderly must put back the container at its holder (Fig. 21).

ThingSpeak bar graph for analysis ThingSpeak bar graph is used to ease the further analysis step done by the doctors or caretaker if they need to monitor the medication time of the elderly (Fig. 22).

Data stored in ThingSpeak This show some of the data stored in ThingSpeak before it is shown in the bar graph. The excel data prove that the automated pill dispenser does drop the medication within the six hours-time intervals (Fig. 23).

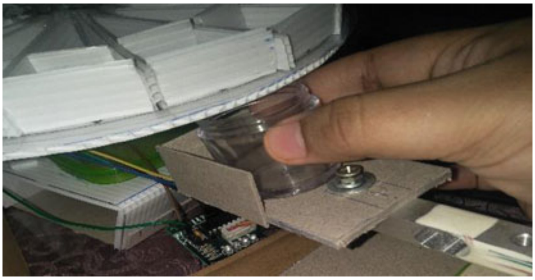


Fig. 21 Pill container is put back in

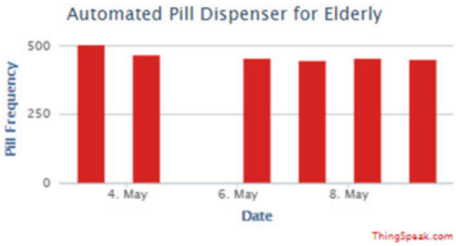
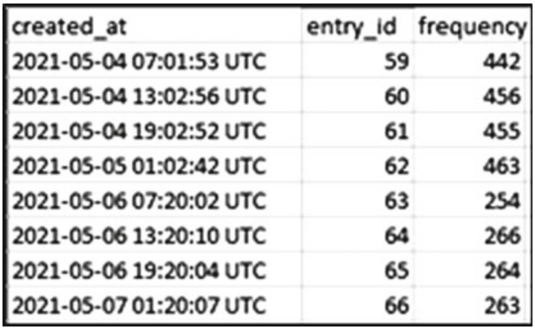


Fig. 22 Bar graph shows the frequency of medication drop for the automated pill dispenser



created_at	entry_id	frequency
2021-05-04 07:01:53 UTC	59	442
2021-05-04 13:02:56 UTC	60	456
2021-05-04 19:02:52 UTC	61	455
2021-05-05 01:02:42 UTC	62	463
2021-05-06 07:20:02 UTC	63	254
2021-05-06 13:20:10 UTC	64	266
2021-05-06 19:20:04 UTC	65	264
2021-05-07 01:20:07 UTC	66	263

Fig. 23 Excel data from ThingSpeak

4.2 Discussion

After finishing the user testing of the paper, some discussions were resolved. One of the discussions is that each pill is varied in sizes and weight, so the compartment size should not be too small in case the elderly consumes bigger capsule compared to the tested pills.

Next, the minimum weight that could trigger the system is 1.00 mg, so anything with a lesser weight than the minimum weight might not trigger the system. But, research done by Barret [2] stated that the elderly taken four pills on average for a daily prescription, so this issue is not a problem as these pills already exceed the minimum weight set for the weight sensor.

5 Conclusion and Recommendation

5.1 Conclusion

In conclusion, this device is very beneficial in eliminating the risk of overdose and underdose, especially among the elderly. The caretakers can ease their worries in case they need to stay away from the elderly and cannot monitor the medication schedule of the elderly. The alerts on the hardware and also notification that run simultaneously helps in the monitoring process and medication intake. The doctors or health researchers could analyze the data taken if there are any issue of prescribed medications to the elderly.

5.2 Recommendation

As for the future developers, they could consider fabricating a portable design of the device as it helps in making its' feature more reliable. Next, temperature and humidity sensors are advisable to be included in future recommendations as they can ensure the level of quality of the medication. These sensors are very beneficial in maintaining the medication's quality as the pills are taken out from their case earlier than consumption time. Finally, next developers can include camera features as a precaution to make sure that the elderly are taken their medication on time. This will eliminate the issue of the elderly might throw their medication away.

References

1. Arora K, Singh U (2018) Smart pill dispenser using internet of things. Int J Eng Res Technol 7(7):48
2. Barret L (2005) Prescription drug use among midlife and older Americans. AARP (2005)
3. Dumanskiy D (2020) blynkkk/blynk-server. GitHub
4. Jayamani S, Mohanram D, Nandhakumaran L, Nila T, Nivetha S (2020) Automatic pill dispenser and consumption monitoring system. Int J Res Eng Sci Manage 3(4):647–649
5. Jayanthi S, Sindhuja S, Sariga S, Hemamalini A, Pavithra G, Priya R (2020) Smart pill dispenser. J Critical Rev 7(8):481–1481
6. Luuk I (2020) 4-Wire load cell (1/5/10/20/200kg) with HX711 and Arduino. Circ J
7. Omega. https://www.omega.com/en-us/resources/load-cells. Last accessed 1 Nov 2021
8. Sahlab N, Sailer C, Jazdi N, Weyrich M (2020) Designing an elderly-appropriate voice control for a pill dispenser. AUTOMED—Autom Med Eng
9. Salzman C (2015) Medication compliance in the elderly. Pubmed (2015)
10. Shaji S (2020) Arduino Mega V3 specification. Tomson Electronics
11. Sharma M (2019) The iterative waterfall model. Includehelp
12. Sumant O, Thakur A (2020) Automatic pill dispenser machine market size & share by 2023. Allied Market Research
13. Yugandhar V, Jayanthi S (2020) Design of virtual pill box and alerting for healthcare monitoring system. J Crit Rev 7(6):1998–2000

Android Malware Classification Addressing Repackaged Entities by the Evaluation of Static Features and Multiple Machine Learning Algorithms

Md Rashedul Hasan

Abstract Expanded usage and prevalence of android apps allows developers of malware to create new ways in various applications to unleash malware in various packaged types. This malware causes various leakage of information and a loss of revenue. In addition, the discovered software is repeatedly launched by unethical developers after classifying the program as malware. Unluckily, the program still remains undetected even after being repackaged. In this research, the topic of repackaging was discussed, emphasizing the implementation based on source code using the bag-of-words algorithm and testing the findings through machine learning. The findings of the assessment demonstrate comparatively improved result in this aspect than the existing implantation based on source code by adapting the bag-of-words strategy and implementing some supplementary dataset preprocessing. A vocabulary for identifying the malicious code has been developed in this study. Bag-of-words was used to classify malware trends using custom implementation. The findings were instantiated using various algorithms of machine learning. The concept was eventually implemented in a practical application too. The suggested method sets out a fairly new methodology for examining source code for android malware to tackle repackaging of malware.

Keywords Android · Malware analysis · Bag-of-words · Source transliteration

1 Introduction

The world is being tethered at a rapid rate with a growing number of mobile devices. Because of the volume of sensitive information stored on or accessible through these devices, cyber-criminals have consider them to be an appealing target, as people are not aware about the attack surface here [1]. It has been discerned; however, the conventional security methods in regular environments are often not appropriately executed by software developers, which may result in considerable security issues.

M. R. Hasan (✉)
Cybertrendz Inc., Dhaka, Bangladesh
e-mail: rashedhasan090@gmail.com; rashed@cybertrendz-inc.com

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_3

Who is unable to realize a security architecture focused on android authorization offers protection to a lesser extent about device authorization [2]. Numerous malware instances have been distributed through the Google Play Store, one of the main places for users to access applications for android [3]. Again, malware source code repackaging increases the possibility and likelihood of malware being released in various variants. The reasons for this are desperately needed to make a case for greater efficiency in malware analysis. According to conclusive research, malware detection engines detect malicious activities only when an application is properly packaged and assembled, not when it is in raw state. For example, if an antivirus engine discovers a malicious APK file, the developer may disassemble that apk file in order to obtain the core source files and gather a set amount of capabilities from those source files before implementing them in a different .apk file so that it is not detected. The form of source code in another file has been altered in a different format and is not considered malicious although previously it is used for malicious activities like espionage on call record or SMS collection. A new Apk file for android is launched with the same source code avoiding antivirus detection. Which means, even the apk was changed the malicious source code was re used. This initiates a sense of when raw source code is being re used in another form of .apk file - the risk of exploitation still remains. The attacker just has changed the name and some basic segments. But the source code is still malicious.

That is a serious problem that must be addressed. In order to find a plausible solution, therefore, the research was focused on this specific field.

The goals to achieve the target are as follows:

a. Propose a relatively newer form of static analysis to help identify and reference precision for a specific field work.
b. Propose and implement an efficient methodology that inclines static analysis technique to acknowledge repackaging.
c. Understand the efficiency and accuracy of the suggested methodology, the text processing algorithm bag-of-words is to be modified using static analysis and machine learning, which would result in a wordlist of harmful phenomena.
d. Make an assessment of the model by the means of different machine learning algorithms.
e. Implementation of the model in a practical form. For this research, Python raw code was utilized as few tools like JD-gui, Dex to jar were also utilized. In addition PHP, HTML, CSS, and MySQL database has been instantiated the Web version of the suggested model.

2 Literature Review

Android operating system and networking technologies are becoming increasingly popular, as the android platform's features (open source, third-party device market support, etc.) which cause the incredible speed of android malware pose a significant threat to this platform [4]. The traditional methods to mobile malware detection sought to identify battery usage anomalies [5]. Malware detection methods that are adaptable might include server working occurrences such as object locks, i/o requests with API calls, and object locks. For example, Malware detection was conducted from network traffic generated from wireless access points by analyzing data [6]. Researchers have developed an anomaly-based malware detection system. This research is addressed as AMD-EC, an entropy-based anomaly detection methodology that detects android malware with an ensemble classifier composed of many one-class classifiers [7]. The detection of static malware is expected to reduce experimental speed and interoperability since manual procedures find techniques. Many strategies for streamlining the static assessment process also have been incorporated. Extensive methods to check program operation are suggested by researchers to turn the malware source code into CCS declarations [8]. Dynamic fingerprinting has been used by the authors proposed a framework—DySign, which signifies the computation of signatures and behavior patterns during dynamic response to ensure responsiveness to slight changes in the behavior of potential variants of malware [9]. Other research, on the other hand, involves conventional machine learning approaches such as SVM, perception, and decision trees [10]. The author of NIDS proposed an efficient, real-time detection, and classification of network behavior-based malware employing deep neural networks. The results illustrate that partitioning the system into two neural networks, detection and analysis, is the key for enhancing precision. As a result, this mechanism facilitates the generation of an in-house monitoring system that consumes extremely little CPU power [11]. Researchers in GRAMAC developed a system where the graph fingerprint of a new application is contrasted to the graph fingerprints in the dataset and the application is either classified into the respective malware family or designated as goodware/undiscovered [12]. In their research—the authors [13] have incorporated an android malware detection model. It was a lightweight, computer-intensive solution for different cell phones. They have also created a novel machine learning-based code evaluation methodology. The work mostly concentrated on source code analysis with a focus on permissions for android. In their source code-based technique, accuracy of the results was attained using numerous methods; however, the source code base approach failed to properly address repackaging concept. The source code strategy consisted on M0Droid-featured extracting functions from raw source code and processing them with the bag-of-words algorithm, where any feature was retrieved from that dataset to establish a dataset [14]. Malware repackaging is a significant problem in which a malware's raw source code is reused as otherwise. Android malware which is in packaged form antivirus can detect it easily, but when it is raw, it escapes detection. To solve the problem, we developed a relatively newer approach to address the issue of repackaging in our research paper [15]. In our research paper, we customized the bag-of-words approach to detect the raw source code even it was repackaged. In addition, we identified 69 malicious patterns and implemented the model as a Web-based tool [15]. This research work is a consecutive work for [15], where I was the First author. That previous work actually used SVM machine learning model. This reserach work is an extended verison of the previous work. However, I particularly focused on extending the previous research to discover more malicious patterns to develop our model further by the means of different machine learning algorithms and newer patterns in the source code based on the previous model. So, the goal was to improve the model of malware repackaging by the means of static analysis procedure complimented with multiple machine learning algorithms which was previously assessed with a single algorithm.

3 Methodology

The whole study was split into few subsections. To begin by considering research work that was already commenced, rework on the generalized bag-of-words algorithm and give better accuracy to a changed model. Secondly, create a sequence of words or list of malicious code or keywords. Our previous work regarding source code repackage model [15] has been considered as the basis of this because the main agenda was to perform malware analysis with raw source code, as it dealt with the problem of repackaging. This is a key concern, and the if model can perform more accurately, it would provide better accuracy on practical implementation.

3.1 Method Representation

In this study, jar is converted from .dex file, then to class to obtain Java code, and Java codes are merged to process the bag-of-word algorithm and a dataset to be produced to apply machine learning technique to the set. The premise for this research has been to engage with the evaluation process employing raw source code, where it has been converted to .zip file format and following the format to raw source code. The proposed model is shown in Fig. 1. The .apk files were obtained from the M0Droid dataset in relation to the base paper. The M0droid dataset contained system calls and package names. As like the work driven in the base paper, source code from all 368 files was extracted. This process has been done by collecting .apk files according to the dataset for M0droid. Then, .apk files have then been translated into zip format and concurrent core .dex files named classes .dex had been retrieved. In this approach, the analysis of the dex file via VirusTotal is suggested, and the core file with the VT graph identifies the central infection position [16]. A windows-based tool dex-to-jar was used to obtain the .jar file, and Java files were separated with another windows-based tool, jd-gui. In order to achieve better results, a modification of bag-of-words was applied, and malicious patterns were classified via a custom filtering method utilizing a supervisory version of the algorithm to combine Java codes only from infected files for dataset.

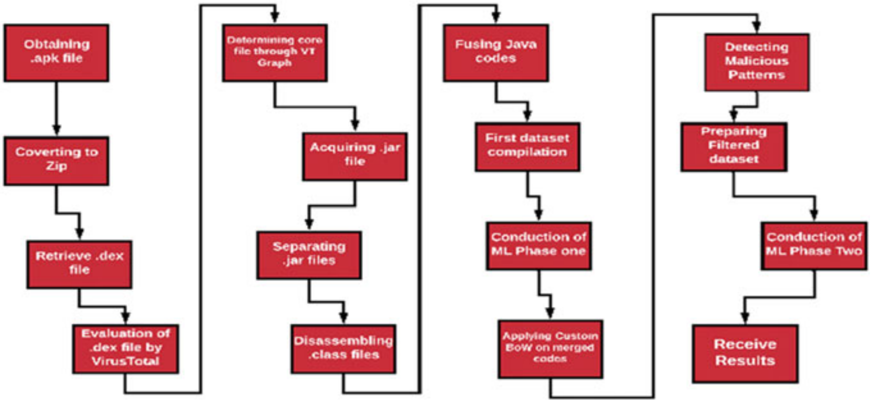

Obtaining .apk file
Coverting to Zip
Retrieve .dex file
Evaluation of .dex file by VirusTotal
Determining core file through VT Graph
Acquiring .jar file
Separating .jar files
Disassembling .class files
Fusing Java codes
First dataset compilation
Conduction of ML Phase one
Applying Custom BoW on merged codes
Detecting Malicious Patterns
Preparing Filtered dataset
Conduction of ML Phase Two
Receive Results

Fig. 1 Methodology

Another filtered dateset has been developed to perform machine learning on the dataset from the apprehension of the modified bag-of-words algorithm. The methodology is given in Fig. 1. They were sent online to VirusTotal after receiving the .dex files. It analyzes the .dex files and provides its status results on the basis of the VirusTotal antivirus engines. The VT graph, a distinguishing trait of VirusTotal, illustrates the precise location of the infected file. Upon the exact location of the file, .Java files were only combined for the first dataset from that specific region. In this research papers, the source code was used to construct a dataset, and the bag-of-words algorithm was used, but additional preprocessing for the final dataset was performed in this research which is one of the major contribution of this research. Since certain keywords and library functions can never be deemed as malicious, they were excluded from such criteria. In addition in this study, the bag-of-word algorithm was used before the separation of fresh as well as malicious keywords. Stop words such as default file names, variable, keywords, alongside with space gaps, and special characters were considered as new keywords. Malicious source codes for Java system calls, packages, and methods were obtained through the effort of various researchers. API call information was collected from the work in [17]. Function references were obtained from [18]. There have again therefore been classes from the android malware detection evaluation features [19]. GroddDroid provided a series of malicious classes which was obtained from that research [20]. Different references contributed around 70 malicious patterns in different cases. For the rest, the function, methods, and classes of the malicious source code detected by VirusTotal were inspected and separated manually for possible Java API calls.

3.2 Customization and Utilization of Bag-of-Words Algorithm

Bag-of-words model is fundamentally a NLP technique for extracting text features or perhaps words from sentences [21]. The implementation accounts for the abundance of words in a record. After reviewing the mainstream algorithm and its use in prior research works, it was determined to modify the algorithm for the proposed model. In particular, three segments have been modified so that they can be addressed sequentially:

Data Collection Process

The intended vocabulary is focused about comparing each line. The quotation marks and comma should be the minimum for each line. Thus, to check each line of the code sequentially, a Python script was developed. While the script would be concluded, an output file would be produced.

Vocabulary Development and Management

After reviewing the basic bag-of-words algorithm, it was modified according to the need of this research works agenda. It consists of three segments—tokenization, extracting words from phrases, and developing a bag-of-words format. The script was created used with Python modules such as NumPy and Re. Words from sentences where words that are not present in vocabulary are overlooked would be removed. The text that has been cleaned which appeared in the body for the tokenization. Sorting of words were conducted afterward. Based on the given input, the source codes were generated.

Counting Mechanism

When a word is available, it is depicted as a 1 in the matrix that equates to the presence of its term in the total vocabulary; when the presence is not identified, it is then denoted as 0. In this circumstance, the vocabulary comprised the majority of the harmful keywords, making it easy to categorize them.

Malicious Keywords Categorization

The properties of malicious code patterns discovered in diverse study materials are used to classify them. Malicious terms were classified with some identifiers, such as privacy-based API calls. API calls on SMS, API calls on Wi-Fi, functions, classes based on SMS, classes based on telephony, classes based on security and few other classes, methods, and call requests. Following this strategy, a variety of small keywords were appended to the dictionary in order to determine a call requests, dataset functions as well as numerous method in VirusTotal tests. These were carefully selected and examined from the source code of the malware versions. If found, they were added into the dictionary. Around 70 types of patterns from different references were utilized for this categorization.

4 Result and Discussion

The sample source codes for 368 specimens were decompiled accordingly, as mentioned before the M0Droid dataset acted as a source from where application packages are extracted and collected. Both datasets have indeed been developed on this basis. For evaluating the dataset, few algorithms like SVM, decision tree, random forest, logistic regression, and multinomial Naïve Bayes were used. A dataset was then created. The two step compilation and assessment was conducted based on the mentioned process in methodology. Here, it is shown that the accuracy is predominantly around 95.65% availing a precision, recall with F1-score of 0.5. This indicates that the change process or additional preprocessing of the bag-of-word algorithm made on this research is reliable (Table 1).

The previous model with similar instantiation obtained, it is the comparative result for source code-based classification based on SVM—which was 95.65%. Comparison with the existing results on SVM-based implementation indicates, this research has a better accuracy on SVM with a 96.42% of accuracy (Table 2).

As mentioned previously, this modified model performs relatively better, so the following 14 keywords have been added to the existing vocabulary list by examining the dataset. Whereas, the previous model was based on 12 malicious keywords. The list of keywords added to the current dictionary is shown in Table 3. These keywords were identified with malicious code segments while complimenting them on malicious activities.

These fourteen words can be marked as a finding of this research which would assist to identify more such malicious patterns.

In addition, a framework for testing has already been designed. The program functions as follows: Any source code from the Java platform can be copied here and pasted here in every android application. The “Review Source” button is to send it. When using the trained language, the machine tests it. If the corresponding

Table 1 ML results from the final dataset

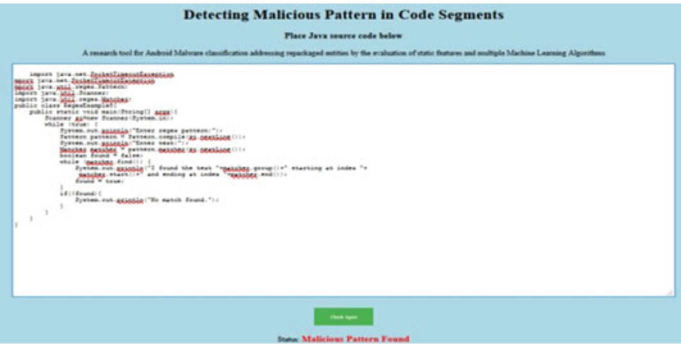
Algorithm	Accuracy (%)	Precision	Recall	F1
SVM	96.42	0.5	0.5	0.5
Decision Tree	94.46	0.44	0.5	0.48
Random Forest	92.67	0.6	0.5	0.565
Logistic Regression	95.61	0.7	0.7	0.7
Multinomial NB	95.65	0.5	0.5	0.5

Table 2 Results comparison

Parameters	Existing model	Proposed model	Comparison
Algorithm	SVM	SVM	0.77% better
Accuracy	95.65	96.42	

Table 3 Keywords obtained from external observation

Collected entities from observation
MessagesContentSender(), fetchContact(), GetappInfo() IMAdTrackerReceiver(), IMAdLocationTracker(), onStartCommand(), onTerminate(), PendingIntent.getService(), InstallActivity.this.startActivity(), getPassword(), getSession(), getPasswordAuthentication(), fetchContacts(), Android.telephony.phoneStateListener



Detecting Malicious Pattern in Code Segments

Place Java source code below

A research tool for Android Malware classification addressing repackaged entities by the evaluation of static features and multiple Machine Learning Algorithms

```
    import java.net.SocketTimeoutException;
import java.net.SocketTimeoutException;
import java.util.regex.Pattern;
import java.util.Scanner;
import java.util.regex.Matcher;
public class RegexExample{
    public static void main(String[] args){
        Scanner sc=new Scanner(System.in);
        while (true) {
            System.out.println("Enter regex pattern:");
            Pattern pattern = Pattern.compile(sc.nextLine());
            System.out.println("Enter text:");
            Matcher matcher = pattern.matcher(sc.nextLine());
            boolean found = false;
            while (matcher.find()) {
                System.out.println("I found the text "+matcher.group()+" starting at index "+
                 matcher.start()+" and ending at index "+matcher.end());
                found = true;
            }
            if(!found){
                System.out.println("No match found.");
            }
        }
    }
}
```

Status: Malicious Pattern Found

Fig. 2 Detecting malicious pattern

vocabulary was found, then it would appear to be vulnerable otherwise not vulnerable (Fig. 2).

5 Conclusion and Future Research Direction

The effort focuses very much on distributive static analysis process and preventing malicious source code to be repackaged. Current research in the field does not provide a model for the scheme that can deliver better productivity and precise performance. The model proposed deals correctly with the issue of repackaging. Standard static analysis does not answer the main purpose of the study properly. Another aim was to represent its effectiveness with the application of the classification algorithm SVM. This research has utilized few algorithms like SVM, random forest, decision tree, logistic regression, and multinomial Naïve Bayes. Instead of few fixed-define properties which were observed in similar research, this approach focused on different characteristics of source code in general and specialized forms to detect malicious patterns. In comparison to a similar classification-based adaptation to the source code, the proposed model has achieved 0.77% better accuracy than our previous existing implementations.

In addition, this work has introduced to the vocabulary 14 more malicious trends that allow the vulnerable android application to be repackaged. This study demonstrates a method for checking the pattern of malicious android source code application while repackaging. This program helps to assess whether a particular piece of code is malicious based on the implemented pattern structure. In the future, this research can be improved by adding more malicious vocabulary patterns. The proposed model was applied as a Web-based framework in practice and can readily be applied to malware detection engines on a large scale.

Acknowledgements Co-authors of this previous research stated in [15] had good contribution for assessment of the identification of the core issue, which laid groundwork for this consecutive research work. Additionally, Associate Dean of the Faculty of Science and Information Technology (FSIT) of Daffodil International University—Prof. Dr. Md. Fokhray Hossain has always inspired me to continue my research in the intended field after my graduation from Daffodil International University.

References

1. Chia C, Choo K, Fehrenbacher D (2017) How cyber-savvy are older mobile device users?
2. Alavi A, Quach A, Zhang H, Marsh B, Haq F, Qian Z, Lu L, Gupta R (2017) Where is the weakest link? A study on security discrepancies between android apps and their website counterparts
3. Hutchinson S, Karabiyik U (2019) Forensic analysis of spy applications in android devices. [online] Scholarly Commons. Available at: https://commons.erau.edu/adfsl/2019/paperpresentation/3/
4. Sharmeen S, Huda S, Abawajy JH, Ismail WN, Hassan MM (2018) Malware threats and detection for industrial mobile-IoT networks. IEEE Access 6:15941–15957. https://doi.org/10.1109/access.2018.2815660
5. Buennemeyer TK, Nelson TM, Clagett LM, Dunning JP, Marchany RC, Tront JG (2008) Mobile device profiling and intrusion detection using smart batteries. In: Proceedings of the 41st annual hawaii international conference on system sciences (HICSS 2008). https://doi.org/10.1109/hicss.2008.319
6. Wang S, Chen Z, Yan Q, Yang B, Peng L, Jia Z (2019) A mobile malware detection method using behavior features in network traffic. J Netw Comput Appl 133:15–25. https://doi.org/10.1016/j.jnca.2018.12.014
7. Ghaffari F, Abadi M, Tajoddin A (2017) AMD-EC: anomalybased Android malware detection using ensemble classifiers. In: 2017 Iranian conference on electrical engineering (ICEE). https://doi.org/10.1109/iraniancee.2017.7985436
8. Mercaldo F, Nardone V, Santone A, Visaggio CA (2016) Download malware? No, thanks. In: Proceedings of the 4th FME workshop on formal methods in software engineering
9. Karbab EB, Debbabi M, Alrabaee S, Mouheb D (2016) DySign: dynamic fingerprinting for the automatic detection of android malware. In: 2016 11th international conference on malicious and unwanted software (MALWARE). https://doi.org/10.1109/malware.2016.7888739
10. Nath HV, Mehtre BM (2014) Static malware analysis using machine learning methods. In: Recent trends in computer networks with distributed systems security. Communications in computer and information science, pp 440–450.https://doi.org/10.1007/978-3-642-54525-2_39
11. Al-Maksousy HH, Weigle MC, Wang C (2018) NIDS: neural network oriented intrusion detection system. In: 2018 IEEE international symposium on technologies for homeland security (HST). https://doi.org/10.1109/ths.2018.8574174
12. Vij D, Balachandran V, Thomas T, Surendran R (2020) Gramac. In: Proceedings of the tenth ACM conference on data and application security and privacy. https://doi.org/10.1145/3374664.3379530

13. Milosevic N, Dehghantanha A, Choo K-KR (2017) Machine learning aided Android malware classification. Comput Electr Eng 61:266–274. https://doi.org/10.1016/j.compeleceng.2017.02.013
14. Damshenas M, Dehghantanha A, Choo K-KR, Mahmud R (2015) M0Droid: an android behavioral-based malware detection model. J Inf Privacy Secur 11(3):141–157. https://doi.org/10.1080/15536548.2015.1073510
15. Hasan MR, Begum A, Zamal FB, Rawshan L, Bhuiyan T (2020) Android malware detection by machine learning apprehension and static feature characterization. In: Bhuiyan T, Rahman M, Ali M (eds) Cyber security and computer science. ICONCS 2020. Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering, vol 325. Springer, Cham. https://doi.org/10.1007/978-3-030-52856-0_5
16. VirusTotal (n.d.) Retrieved from https://www.virustotal.com/
17. Chan PPK, Song W-K (2014) Static detection of Android malware by using permissions and API calls. In: 2014 international conference on machine learning and cybernetics. https://doi.org/10.1109/icmlc.2014.7009096
18. Patanaik CK, Barbhuiya FA, Nandi S (2012). Obfuscated malware detection based on API call dependency. In: Proceedings of the first international conference on security of internet of things—SecurIT 12. https://doi.org/10.1145/2490428.2490454
19. Leeds M, Keffeler M, Atkison T (2017) A comparison of features for android malware detection. In: Proceedings of the SouthEast Conference on— ACM SE 17.https://doi.org/10.1145/3077286.3077288
20. Abraham A, Andriatsimandefitra R, Brunelat A, Lalande J-F, Tong VVT (2015) GroddDroid: a gorilla for triggering malicious behaviors. In: 2015 10th international conference on malicious and unwanted software (MALWARE). https://doi.org/10.1109/malware.2015.7413692
21. Bag-of-words model (2019, November 29) Retrieved from https://en.wikipedia.org/wiki/Bag-of-words_model

Enterprise Architecture Quality Assessment

Małgorzata Pańkowska

Abstract The enterprise architecture (EA) assessment can be provided in different ways. In general, the EA assessment supports information communication technology (ICT) implementation. Beyond that, business organization stakeholders have an opportunity to monitor effectiveness and efficiency of business processes. They can modify the business structure, increase the business innovativeness, and ensure business strategy realization. Nowadays, EA stakeholders establish their own methodologies for EA quality assessment. This paper includes analyzes of the architecture frameworks, assessment models, and standards. This article aims to answer the question, if the design science research (DSR) paradigm is useful for EA quality assessment. Hence, this paper includes a proposal of new approach to EA quality assessment, based on emphasizing the relevance and rigor as key concepts.

Keywords Enterprise architecture · Design science research · Relevance · Rigor · Quality assessment · ISO 42030 standard

1 Introduction

The term "enterprise" can be understood as an overall idea to identify a production company, business organization, or governmental institution [1]. The enterprise architecture (EA) is defined as a coherent set of artifacts, rules, principles, norms, standards, and guidelines that guide computerized information system design and implementation [2]. The enterprise architecture as a process of translating business vision and strategy into effective enterprise can be viewed in many different aspects, i.e., business, information, work, software application, and technology [3, 4].

The EA assessment refers to systematic activities undertaken to make decisions on the quality of particular artifacts and visualize them in a structured way. The EA assessment means decisions on the quality of EA objectives, development activities, information resources, processes, actors, products, requirements, and relationships

M. Pańkowska (✉)
University of Economics in Katowice, Katowice, Poland
e-mail: pank@ue.katowice.pl

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_4

among those artifacts. EA ensures a holistic view of the enterprise's key strategies and their impact on business functions and processes, taking the firm's sourcing goals into explicit considerations. Therefore, EA should be holistically assessed. Popular criteria of assessment are the following: cost efficiency, flexibility, enhancing productivity using less expensive and carefully chosen resources, process simplification, or effectiveness and efficiency of business transactions. The EA stakeholders have different opinions on quality; hence, the EA quality assessment should be presented as multi-criteria decision-making. In this paper, this decision process is based on the DSR paradigm. This research paper is organized as follows. The second section includes discussion on different EA frameworks and EA assessment methods. Next, the ISO standards are analyzed, and some additional methods are presented. In the fourth section, the DSR methodology, relevance, and rigor cycles are considered as important for EA quality assessment. Next, the EA quality attributes are presented and placed in the DSR model. For this study, the literature survey method was applied. In particular, Scopus and Research Gate repositories were reviewed.

2 Enterprise Architecture Frameworks

Nowadays, EA is considered as a research discipline guided with principles, frameworks, methodologies, requirements, tools, reference models, and standards. There are many frameworks that support EA modeling and development, e.g., Unified Architecture Framework (UAF), Zachman Framework (ZF), the Federal Enterprise Architecture Framework (FEAF), the Ministry of Defense Architectural Framework (MODAF), Computer Integrated Manufacturing Open System Architecture (CIMOSA), the Open Group Architecture Framework (TOGAF), the Extended Enterprise Architecture Framework (E2AF), the Department of Defense Architecture Framework (DODAF), the Generic Enterprise Reference Architecture and Methodology (GERAM), Treasury Enterprise Architecture Framework (TEAF), and Adaptive EA [5]. Figure 1 covers the average number of citations per publication on the particular framework of enterprise architecture. This measure can be considered as the academia acceptance metrics. As it is visible in Fig. 1, a huge number of publications does not mean many citations, although Pearson correlation equals 0.895 for data in Table 1.

The unified architecture framework (UAF) is object management group (OMG) standard, which focuses strategic objectives, business processes, organization management, resource allocation, and security. Architecture models are constructed by system modeling language (SysML), as well as by natural language [6]. The ZF provides fundamentals for modeling a business ontology through dimensions such as data, function, network, people, time, and motivation [7]. Each aspect presents the architecture from a particular perspective, and therefore, the quality of each artifact can be assessed separately.

In the FEAF, the performance reference model (PRM) is proposed to measure the performance of major IT investments, as well as the customer service quality, process

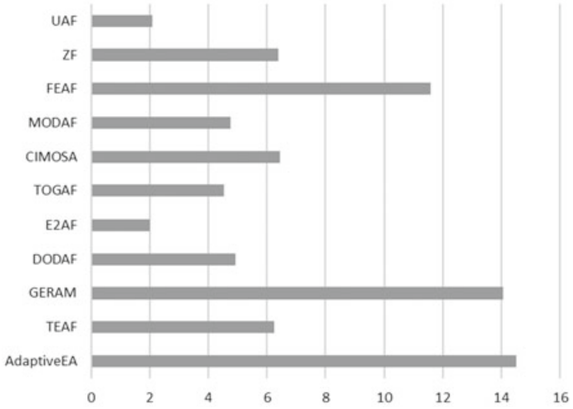


Fig. 1 Average number of citations per publication on the EA framework in Scopus

Table 1 Citations and publications on the EA frameworks in Scopus

Framework	Citations (c)	Publications (p)	Acceptance (c/p)
UAF	25	12	2.08
ZF	1744	273	6.38
FEAF	324	28	11.5
MODAF	285	60	4.75
CIMOSA	271	42	6.45
TOGAF	1346	298	4.52
E2AF	2	1	2
DODAF	1252	254	4.92
GERAM	534	38	14.05
TEAF	25	4	6.25
Adaptive EA	1248	86	14.51

and activity quality, and technology quality [8]. The MODAF framework covers seven viewpoints, i.e., all view, acquisition, strategic, operational, system, service, and technical and the EA artifacts quality can be assessed at each of these aspects [9]. The CIMOSA framework is based on four abstraction views (i.e., function, information, resource, and organization) and three modeling levels (i.e., requirements definition, design, specification, and implementation description) [10]. The four views are provided to manage the integrated enterprise model covering the design, manipulation, and assessment. In TOGAF [11], the holistic approach to the EA quality management is possible through the application of the architecture maturity model (AMM), which is developed to improve architecture processes as well as to assess the organization's competence. High-quality architecture model should be consistent, relevant, and justified.

Van Den Berg and Van Steenbergen consider eighteen key areas of architecture maturity, which can be included in the EA assessment process [12]. Perko is writing about some other commonly known EA maturity models, e.g., NASCIO Enterprise Architecture Maturity Model, A Framework for Assessing and Improving Enterprise Architecture Management (EAMMF), IT Architecture Capability Maturity Model, OMB Enterprise Architecture Assessment Framework, and Extended Enterprise Architecture Maturity Model (E2AMM) [13].

The E2AF framework focuses on integration and cohesion of architecture artifacts [14]. The DODAF framework is developed to ascertain that the architectural components' compatibility and interrelationships, as well as the technical architecture usability and integration across organizational domains [15]. The GERAM is assumed to support an enterprise integration and to ensure that information of adequate quality, and detail is delivered to the management for short- and long-term decision-making [16]. The TEAF framework implements the enterprise architecture roadmap, information assurance risk assessment, and information assurance trust model to support EA quality management. The adaptive enterprise architecture framework promotes business alignment, enterprise agility, as well as non-functional requirements, i.e., reliability, security, or quality of service [17]. The presented EA frameworks include analyzes of architecture models on a high level. The frameworks' developers want to ensure a coherence among different components, their scalability, openness, agility, and sustainability as well as convergence of the proposed models.

3 Enterprise Architecture Evaluation

The business-information technology alignment (BITA) models are applicable for the EA quality assessment [18]. The BITA processes should be conducted periodically to analyze each architectural level to identify technology gaps, identify and assess the current EA state, determine future state, identify metrics to compare current and future states, identify stakeholders, and determine their interests, develop standards, frameworks, and transition plans. Scenario-based architectural evaluation is a structural approach to evaluating how well the architecture meets stakeholders' needs [19, 20].

In literature, the enterprise architecture assessment usually concerns selected aspects of the review, e.g., EA effectiveness assessment [21, 22], EA evaluation process [23]. Khayami [24] proposes the following quality attributes of EA: alignment, convergence, maintainability, integrity, reliability, efficiency, security, and usability. Neimi and Pekkola [25] focus on other attributes, i.e., clarity, granularity, uniformity and cohesion, availability, correctness, and usefulness. Firesmith and Capell [26] propose the quality assessment of system architecture and their requirements (QUASAR) model including external characteristics (e.g., compliance, configurability, or usability) as well as internal (e.g., feasibility, interoperability, reusability, or modifiability). They argue that quality is a degree to which a work product (e.g., system, subsystem, requirement, or architecture) exhibits a desired amount of useful or needed characteristics. Timm [27] argues that reference enterprise architectures (R-EA) help to save costs and increase the EA quality in the regulatory compliance management (RCM) approaches. Escobar et al. [28] propose for the EA quality evaluation the usage of quality characteristics according to the ISO/IEC 25010:2011, where a product quality is characterized by user satisfaction, effectiveness, efficiency, context completeness, and freedom from risk [29]. However, the ISO/IEC/IEEE 42030: 2019 is fundamental for EA quality assessment [30]. This standard emphasizes the necessity of EA evaluations for many reasons, such as the evaluation of an architecture suitability, addressing stakeholders' requirements and expectations, identification of opportunities for improvement, and assessing the progress of architecture development. According to this standard, architecture quality attributes are as follows: coherence, completeness, elegance, hierarchy, modularity, variability, subsetability (i.e., support the production of a subset), conceptual integrity, commonality (i.e., sharing in preplanned ways), durability, utility, beauty, robustness, feasibility, flexibility, verifiability, traceability, and cohesion [30]. Therefore, the architecture relevance is emphasized and evaluated through making a judgment concerning extent to which architecture objectives are achieved and stakeholder interests are satisfied by decisions that affect the architecture artifacts.

4 DSR Applicability for EA Quality Assessment

Design science research (DSR) is a research work paradigm, in which a designer, who is also a researcher, answers questions relevant to human problems via the creation of innovative artifacts, and also contributes new knowledge to knowledge repositories. The designed or created artifacts are both useful and original for understanding the problem at hand and for providing a practical solution. Historically, Simon [31] was the first who undertook research on design science, in particular for research in artificial intelligence discipline. Design research is well applied in many fields including architecture, engineering, education, psychology, management, behavioral science, computer science, or the fine arts (Fig. 2).

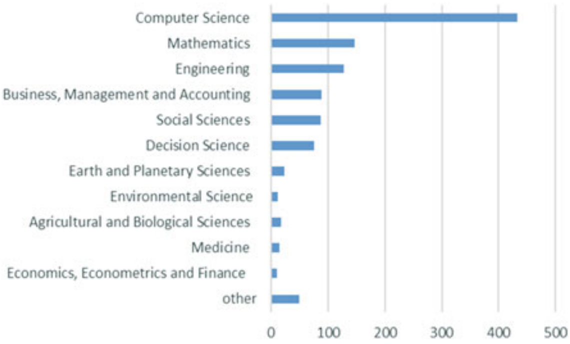


Fig. 2 Volume of publications on DSR in particular disciplines. *Source* Scopus repository

Artifact is a fundamental concept in DSR. Hevner et al. [32, p. 77] identified four types of artifacts:

- Constructs, e.g., concepts formalized in semantic data modeling, conceptualizations, vocabulary, symbols.
- Models, e.g., abstractions, representations, structure of relationships between problem and solution components.
- Methods, e.g., algorithms, practices, or guidelines to perform a task, search the solution space.
- Instantiations, e.g., implemented and prototyped systems.

Andersson [33] argues that constructs represent entities of interest in the theory. Weigand et al. [34] have provided a semantic analysis of artifacts. For them, an artifact can be identified with the research outcome. Goldkuhl and Karlsson [35] define artifact as a human-made object in contrast to a natural object. "Artifact" has its source in the Latin "arte" (i.e., "by skill") and "factum" (i.e., "thing made"). Artifacts are designed to support people in reaching certain planned goals and they function as signs to inform readers, researchers, or engineers. Artifact assessment is necessary to confirm the validity of its contribution. Evidence of artifact utility permits to conclude about further applicability of the artifact. Artifacts are assessed by practitioners, as well as by the academic environment, e.g., project grant donators.

In general, DSR main cycle includes problem awareness, suggestion formulation, development of artifacts, their evaluation, and concluding, where the results are pronounced to be good enough for science and for practice. DSR can be compared to knowledge development through practice, and hence, the action research as qualitative research method is inserted into DSR. Weigand et al. [34] argue that DSR artifacts must keep a certain level of rigor and generalizability, as well as practical and scientific relevance, while generalizability means focus on the reusability and ability to integrate its components. DSR has its origin in pragmatism, where ideas' and theories' value is based on the success of an artifact's practical application [36]. DSR studies are required to maintain a balance between research rigor and practical relevance by reporting artifacts that solve a class of problems. Meyer et al. [37] have presented the DSR application for EA business value assessment. According to them, the design is a search process, where each step requires collaboration of industry partner with researcher to gratify the environmental needs and to adhere to the business requirements. In this approach, problem relevance means satisfying the environmental needs, while research rigor means the usage of adequate methods. Therefore, for the EA quality assessment in DSR, the research question concerns relevance and rigor of artifact development. Barafort et al. [38] define relevance as an alignment of business activities and international standards, industry, and best practices. Mohajeri and Leidner [39] discuss the pluralistic nature of relevance and present a typology of relevance according to four perspectives: applicability, knowledge production transfer, value, and empowerment.

However, this paper suggests to distinguish the academic relevance (i.e., significance, impressiveness, dissemination of results) from practical relevance (e.g., usefulness to practitioners, impact). A given solution can be original, but not applicable nor feasible. Relevance is relative. Relevance is evaluated for academicians, for society, policy, economy, technology, education, or healthcare. Relevance is the degree to which research artifacts contribute to improve the outcomes of interest. On the other side, rigor is a grounding in research methods. Gill and Gill [40] define rigor as criteria-based or compliance-based. Compliance-based perspective is related to the selection of an appropriate research methodology, accurate usage of methods, and documenting that use. Hence, rigor can be identified with competent and systematic usage of procedures, fostering the standardization, audits of reasoning. Rigor in research and also in practice is the strength of reasoning [40], discipline, order, and obedience. The relevance of a research work can be analyzed from two perspectives: the targeted practitioner's perspective and the researcher's perspective. However, rigor is to be also valid for these two environments.

Paine and Delmhorst [41] focus on balance between rigor and relevance. They argue that rigor—relevance balance remains a long-term concern for the enterprise field researchers. Taking into account that rigor and relevance are important for both academia and practice, this study covers a proposal of quality attributes for EA quality assessment. Certain attributes are assumed to be important for practitioners and other for the academia people, i.e., researchers, grant donors, and research process organizers. Figure 3 covers specification of these attributes, which are placed in appropriate fields. Specification of these attributes is based on [42, 43]. Practitioners focus on quality attributes, which enable them to work with the artifacts now and in particular location, and for particular purposes. Academicians seem to be interested in long-term characteristics and abilities to utilize the artifacts in different conditions.

Practice application domain attributes are following (Figs. 3 and 4):

- Availability—the degree to which artifacts are available to all stakeholders on their end-user platforms.

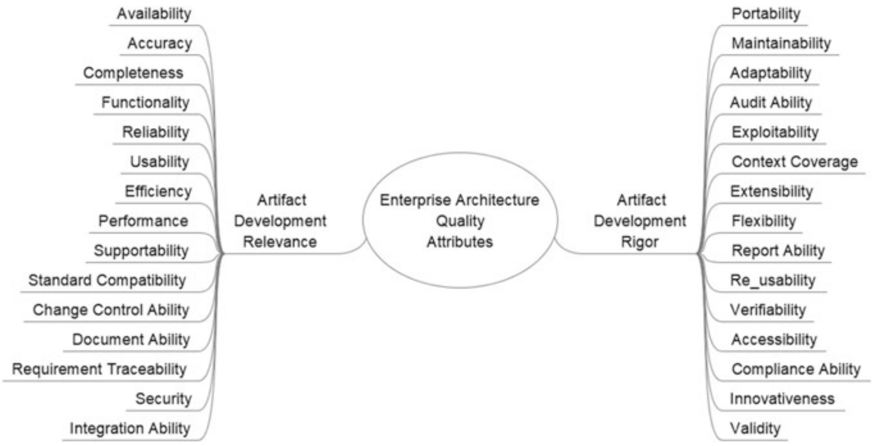


Fig. 3 Enterprise architecture quality attributes

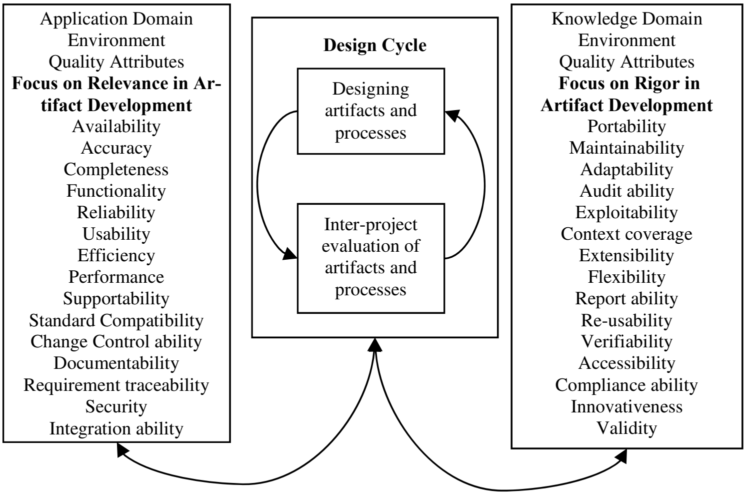


Fig. 4 Adapted DSR paradigm framework for the EA quality assessment

- Accuracy—the degree to which correctly gathered research data define the artifacts.
- Completeness—the degree to which all the artifact data are present.
- Functionality—the degree to which proposed artifacts are useful for further implementation in system functions.
- Reliability—the extent to which the EA system provides a pre-defined level of performance without breaks and errors.
- Usability—the extent to which the EA system is understood and used. The artifact understandability, learnability, operability, and attractiveness are considered.
- Efficiency—the degree to which resources are expended economically and accurately to achieve goals.
- Performance—the grade to which the system ensures a defined level of performance, including process speed, resource usage, capability, and response time.
- Supportability—the extent to which the EA artifacts can be supported by the professionals who have created them.
- Standard Compatibility—the degree to which the artifact is compliant with the EA standards and frameworks.
- Change control ability—the artifact versioning through the EA life cycle, so it is the ability to appropriately manage changes of artifacts.
- Document ability—the degree to which the EA artifacts can be supported by documentary evidence.
- Requirement traceability—the degree to which business functional and non-functional requirements can be traced in the EA development cycle.
- Security—the degree to which unauthorized access to artifacts, including the ability to disseminate data, can be properly protected.

- Integration ability—the ability to bring together artifacts into a cohesive framework that minimizes the duplication of data.

Knowledge domain quality attributes are as follows (Figs. 3 and 4):

- Portability—the degree to which the artifacts can be moved from one environment to another.
- Maintainability—the measured efforts needed to make specified modifications of artifacts.
- Adaptability—the degree to which artifact use open standards that make it easy for artifact components to be interchangeable.
- Audit ability—the degree to which the artifact can be evaluated for properly performing its functionality.
- Exploitability—the degree to which stakeholders can exploit the artifacts for early-unanticipated capabilities.
- Context coverage—the degree to which the artifacts respect the EA context in each particular case.
- Extensibility—the degree to which new artifacts can be added to the whole EA system without loss of cohesion.
- Flexibility—the degree to which the EA can support additional products, workflows, data sources, reports, and analytics.
- Report ability—the degree to which the artifacts are reported to the appropriate stakeholders, administrators, and support staff in a controlled manner with the appropriate set of corresponding data to diagnose and remediate the artifact development.
- Reusability—the degree to which the designed artifacts are highly reusable and easily customizable.
- Verifiability—the degree to which the artifacts can be independently confirmed as being accurate and actual.
- Accessibility—the degree to which the user can promptly access the artifacts in knowledge repositories.
- Compliance ability—the degree to which rules and policies from business, legal agencies, regulatory institutions are adhered to. It is also the degree to which compliance can be traced through the EA life cycle.
- Innovativeness—the creativeness of designers, uniqueness of solution, advantages in comparison with competitive solutions.
- Validity—the degree to which the artifacts are congruent with business rules as well as syntactic and semantic correctness.

5 Illustrative Application of Relevance and Rigor Attributes

Design science research methodology can be applied for information communication technology (ICT) supported innovative projects funded by Horizon Europe Program.

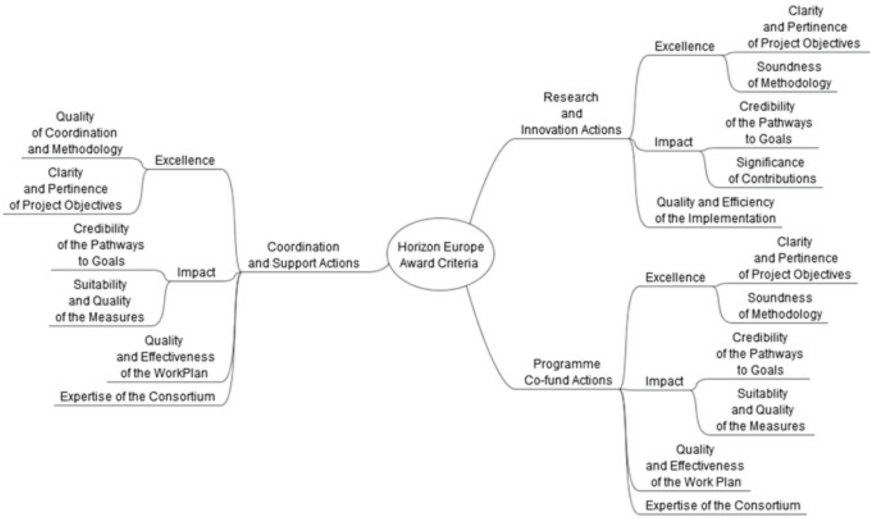

Horizon Europe Award Criteria
Coordination and Support Actions
Excellence
Quality of Coordination and Methodology
Clarity and Pertinence of Project Objectives
Impact
Credibility of the Pathways to Goals
Suitability and Quality of the Measures
Quality and Effectiveness of the WorkPlan
Expertise of the Consortium
Research and Innovation Actions
Excellence
Clarity and Pertinence of Project Objectives
Soundness of Methodology
Impact
Credibility of the Pathways to Goals
Significance of Contributions
Quality and Efficiency of the Implementation
Programme Co-fund Actions
Excellence
Clarity and Pertinence of Project Objectives
Soundness of Methodology
Impact
Credibility of the Pathways to Goals
Suitablity and Quality of the Measures
Quality and Effectiveness of the Work Plan
Expertise of the Consortium

Fig. 5 Horizon Europe innovative solution grant award criteria

Horizon Europe is the European Commission Framework Program following the Horizon 2020 Program. Horizon Europe will run for seven years from 2021 to 2027, and it concerns climate change, sustainable development, and in general, European Union countries competitiveness and growth. The program emphasizes partners' collaboration and strengthens the research and innovation. Therefore, it would be interesting to review what awarding criteria are proposed in Horizon Europe and answer question if they respect the relevance and rigor requirements. This program is assumed to support innovative solutions' development. In many cases, that innovative solutions development needs elaboration of the whole architecture project. The innovative solution is located inside this system architecture. Applicants must elaborate the enterprise architecture to ensure the innovative solution implementation.

Figure 5 includes Horizon Europe Program 2021–2022 award criteria identification according to [44]. The proposed in Horizon Europe Program set of awarding criteria is very general. They are divided into three groups, i.e., excellence, impact, and quality issues. In this way of thinking, the excellence criteria correspond with value of the proposed solution in domain science. Next, the impact criteria are comparable with the relevance criteria in DSR approach, because the relevance is considered as the relevance for practitioners.

European Commission has prepared for small and medium enterprises (SMEs) a separate group of offers. The European Innovation Council (EIC) has been established by the European Commission, under the Horizon Europe Program. The EIC aims at supporting new technologies and game-changing innovations. The EIC program includes three main instruments of financial support. There is the Pathfinder instrument for advanced research on the breakthrough technology. The second is the transition instrument for transforming research results into innovation opportunities,

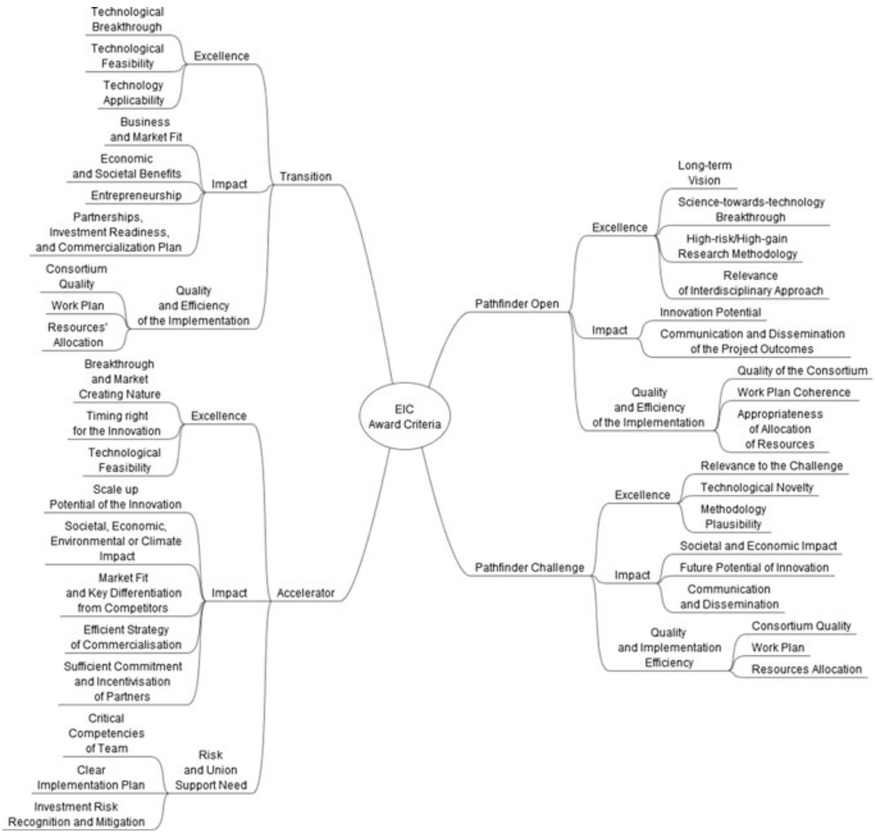

EIC
Award Criteria
Transition
Excellence
Technological Breakthrough
Technological Feasibility
Technology Applicability
Impact
Business and Market Fit
Economic and Societal Benefits
Entrepreneurship
Partnerships, Investment Readiness, and Commercialization Plan
Quality and Efficiency of the Implementation
Consortium Quality
Work Plan
Resources' Allocation
Accelerator
Excellence
Breakthrough and Market Creating Nature
Timing right for the Innovation
Technological Feasibility
Impact
Scale up Potential of the Innovation
Societal, Economic, Environmental or Climate Impact
Market Fit and Key Differentiation from Competitors
Efficient Strategy of Commercialisation
Sufficient Commitment and Incentivisation of Partners
Risk and Union Support Need
Critical Competencies of Team
Clear Implementation Plan
Investment Risk Recognition and Mitigation
Pathfinder Open
Excellence
Long-term Vision
Science-towards-technology Breakthrough
High-risk/High-gain Research Methodology
Relevance of Interdisciplinary Approach
Impact
Innovation Potential
Communication and Dissemination of the Project Outcomes
Quality and Efficiency of the Implementation
Quality of the Consortium
Work Plan Coherence
Appropriateness of Allocation of Resources
Pathfinder Challenge
Excellence
Relevance to the Challenge
Technological Novelty
Methodology Plausibility
Impact
Societal and Economic Impact
Future Potential of Innovation
Communication and Dissemination
Quality and Implementation Efficiency
Consortium Quality
Work Plan
Resources Allocation

Fig. 6 Horizon Europe EIC award criteria

and the third is named the accelerator instrument for companies to develop and scale up innovations with the high risks and high impact. Figure 6 includes European Innovation Council Program award criteria identification according to [45]. There are two main groups of award criteria, i.e., excellence and impact.

The design science research methodology is defined as pragmatic approach. However, the pragmatism is visible also in the Horizon Europe Program. The program projects are expected to be strongly oriented toward actual applicability of the proposed innovative solutions. Relevance to the current societal requirements is emphasized, and rigor concerns effective, efficient, or pragmatic project management.

There is a question if the pragmatism is always effective for knowledge development. The short-term positive effects can dominate, and new ones quickly replace the proposed ICT solutions. When the time to market is important, the applicability and usefulness dominate over other EA characteristics, i.e., internal cohesion, or novelty of IT solutions. The criteria, i.e., originality of research work, strength of arguments, academic soundness, coherence and cohesion of arguments, or way of investigation are typical for evaluation of knowledge contribution. Hence, these arguments could also be considered for an enterprise architecture prototype proposal assessment.

6 Conclusions

As it is presented in literature, the EA benefits cover improved business—IT alignment, better decision-making, reduced IT costs, and increased business performance. The EA development and implementation require time, money, and human efforts. Therefore, business organization capability to assess the quality of the EA artifacts is important. The challenge is to understand how the quality can be measured, because the EA practice produces various artifacts such as models, frameworks, de facto standards, principles, and other descriptive documentation. The degree to which a stakeholder is satisfied with EA depends on the effectiveness of implementation practices. In this article, proposed attributes' specification is to support the EA quality assessment before implementation. The EA artifacts should be assessed as suitable for practice and valid for knowledge and science. The relevance- and rigor-based quality assessment is critical to successful implementation, but on the other side, this approach can support the EA developer and sponsor in their process of the best practices selection for the artifacts development.

References

1. Hoogervorst JAP (2009) Enterprise governance and enterprise engineering. Springer, Berlin
2. Lankhorst M (2005) Enterprise architecture at work. Springer, Berlin
3. CIO Council, Updating the Clinger-Cohen Competencies for Enterprise Architecture (2003). http://www.cio.gov/documents/FINAL_White_Paper_on_EA_v62.doc. Last accessed 15 Jan 2020
4. Op't Land M, Proper E, Waage M, Cloo J, Steghuis C (2009) Enterprise architecture, creating value by informed governance. Springer, Berlin
5. Theuerkorn F (2005) Lightweight enterprise architectures. Auerbach Applications, London
6. Ding Q, Wang Y, Cao G (2020) UAF model verification method based on description logic. IOP Conf Ser Mater Sci Eng 768:072006. https://doi.org/10.1088/1757-899X/768/7/072006
7. Zachman JA (2010) Frameworks standards: what's it all about? In: Kappelman LA (ed) The SIM guide to enterprise architecture. CRC Press, Boca Raton, pp 66–70
8. Minoli D (2008) Enterprise architecture A to Z, frameworks, business process modeling, soa, and infrastructure technology. CRC Press, London
9. Perks C, Beveridge T (2003) Guide to enterprise IT architecture. Springer, New York
10. Spadoni M, Abdmouleh A (2007) Information systems architecture for business process modelling. In: Saha P (ed) Handbook of enterprise systems architecture in practice. Information Science Reference, Hershey, pp 366–382
11. Desfray P, Raymond G (2014) Modeling enterprise architecture with TOGAF a practical guide using uml and BPMN. Elsevier, Amsterdam
12. Van Den Berg M, Van Steenbergen M (2006) Building an enterprise architecture practice, tools, tips, best practices, ready-to-use insights. Springer, Sogeti (2006)

13. Perko J (2008) IT governance and enterprise architecture as prerequisites for assimilation of service-oriented architecture, Tampere University of Technology, Publication 788, Tampere. https://trepo.tuni.fi/bitstream/handle/10024/113959/perko.pdf?sequence=1. Last accessed 20 May 2021
14. Schekkerman J (2006) Extended enterprise architecture, maturity model support guide, version, 2.0. http://docshare04.docshare.tips/files/23487/234876298.pdf. Last accessed 20 May 2021
15. The DoDAF Architecture Framework Version 2.02. (2011). https://dodcio.defense.gov/portals/0/documents/dodaf/dodaf_v2-02_web.pdf. Last accessed 21 July 2021
16. Bernus P, Noran O, Molina A (2014) Enterprise architecture: twenty years of the GERAM framework. IFAC Proc 47(3):3300–3308. https://doi.org/10.3182/20140824-6-ZA-1003.01401lastaccessed2021/05/20
17. Masuda Y, Shirasaka S, Yamamoto S, Hardjono T (2017) An adaptive enterprise architecture framework and implementation: towards global enterprises in the era of cloud/mobile IT/digital IT. Int J Enterp Inf Syst 13(3):1–22. https://doi.org/10.4018/ijeis.2017070101
18. Van Grembergen W (2004) Strategies for information technology governance. Information Science Reference, IGP, Hershey, PA
19. Mekawy ME, Rusu L, Ahmed N (2009) Business and IT alignment: an evaluation of strategic alignment models. In: Lytras MD, Ordonez de Pablos P, Damiani E, Avison D, Naeve A, Horner DG (eds) Best practices for the knowledge society, knowledge, learning, development and technology for all. Springer Berlin Heidelberg, pp 447–455
20. Rozanski N, Woods E (2012) Software systems architecture. Addison Wesley, Upper Saddle River
21. Buchanan R (2001) Assessing enterprise architecture program value: Part 2: META Group Report. Stamford CT
22. Rouhani BD, Nikpay F, Mohamaddoust R (2014) Critical success factors of enterprise architecture implementation. Int J Comput Inf Technol (IJOCIT) 2(1):331–340
23. Nikpay F, Ahmad R, Kia CY (2017) A hybrid method for evaluating enterprise architecture Implementation. Eval Program Plann 60:1–16
24. Khayami R (2011) Qualitative characteristics of enterprise architecture. Procedia Computer Science 3:1277–1282
25. Neimi E, Pekkola S (2013) Enterprise architecture quality attributes: a case study. In: 46th Hawaii international conference on system sciences
26. Firesmith DG, Capell PC (2007) Quality assessment of system architecture and their requirements (QUASAR). J Integr Des Process Sci 11(2):15–31
27. Timm F (2018) An application design for reference enterprise architecture models. In: Matulevicius R, Dijkman R (eds) Advanced information systems engineering workshops. CAiSE 2018. Lecture notes in business information processing, vol 316. Springer, Cham, pp. 209–221. https://doi.org/10.1007/978-3-319-92898-2_18
28. Escobar J, Losavio F, Ortega D (2013) Standard quality model to Enterprise Architecture support tools. In: Proceedings of the 39th Latin American computing conference, CLEI 2013. 50–61 (2013). https://www.researchgate.net/publication/261339832_Standard_quality_model_to_Enterprise_Architecture_support_tools. Last accessed 20 May 2020
29. ISO/IEC 25010:2011 Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and software quality models. https://www.iso.org/standard/35733.html. Last accessed 20 May 2021
30. ISO/IEC/IEEE 42030:2019 Software, systems and enterprise—architecture evaluation framework. https://www.iso.org/standard/73436.html. Last accessed 20 May 2021
31. Simon HA (1996) The sciences of the artificial. The MIT Press, Cambridge
32. Hevner AR, March ST, Park J, Ram S (2004) Design science in information systems research. MIS Q 28(1):75–106
33. Andersson B (2011) Harnessing handheld computing—managing IS support to the digital ranger with defensive design. In: Jain H, Sinha AP, Vitharana P (eds) Service-oriented perspective in design science research. Springer, Heidelberg, pp 62–75

34. Weigand H, Johannesson P, Andersson B (2021) An artifact ontology for design science research. Data Knowl Eng 133(101878):1–19. https://doi.org/10.1016/j.datak.2021.101878
35. Goldkuhl G, Karlsson F (2020) Method engineering as design science. J Assoc Inf Syst 21(5):1237–1278
36. Janse van Rensburg JT, Goede R (2019) A model for improving knowledge generation in design science research through reflective practice. Electron J Bus Res Methods 17(4):192–211
37. Meyer M, Helfert M, Donnellan B, Kenneally J (2012) Applying design science research for enterprise architecture business value assessments. In: Peffers K, Rothenberger M, Kuechler B (eds) DESRIST 2012, LNCS 7286. Springer, Berlin, pp 108–121
38. Barafort B, Shrestha A, Cortina S, Renault A (2018) A software artefact to support standard-based process assessment: evolution of the TIPA. Comput Stand Interfaces 60:37–47
39. Mohajeri K, Leidner D (2017) Towards a typology of relevance. In: Bui T (ed) Proceedings 50th Hawaii international conference system Science. AIS Electronic Library, Atlanta, pp 5783–5792
40. Gill TG, Gill TR (2020) What is research rigor? Lessons for a transdiscipline. Inf Sci 23:47–76
41. Paine JW, Delmhorst F (2020) A balance of rigor and relevance: engaged scholarship in organizational change. J Appl Behav Sci 56(4):437–461
42. Luisi JV (2014) Pragmatic enterprise architecture, strategies to transform information systems in the era of big data. Elsevier, Amsterdam
43. Mistrik I, Bahsoon R, Eeles P, Roshandel R, Stal M (2014) Relating system quality and software architecture. Elsevier, Amsterdam
44. Horizon Europe Work Programme 2021–2022, 13. General Annexes. European Commission Decision C, 1940 of 31 March 2021 (2021). https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-13-general-annexes_horizon-2021-2022_en.pdf. Last accessed 20 Aug 2021
45. EIC Work Programme 2021, European Innovation Council, European Commission Decision C of 17 March 2021 (2021). https://eic.ec.europa.eu/eic-funding-opportunities/eic-accelerator_en#ecl-inpage-137. Last accessed 20 Aug 2021

Planning Rendezvous for Interplanetary Trajectories

Aziz Anouar and Mohammed Bennani

Abstract Great interests are always brought by the scientific community for the exploration of the solar system. Thus, important efforts are to be furnished to this goal. This paper aims to develop an approach of making rendezvous for the planets in the solar system as well as for a big asteroid. All the necessary equations are established by distinguishing the inside and the outside planets orbits relative to the earth. After that a simulation for the departure, the waiting time and the return trip are elaborated. This is followed obviously by an evaluation and comparison of the trip duration for each planet in the solar system. These simulation results would be without doubt very useful in the elaboration of the rendezvous planning strategies.

Keywords Solar system · Planning · Rendezvous · Asteroid · Trip duration

1 Introduction

The exploration of the solar system still interests many fields of the scientific research such as astrophysics, biology, celestial mechanics, engineering sciences, and others. The aims concern essentially the discovery of the richness, variety of the physical and phenomenon in the planets, the research of life, outside the earth, the comprehension of the solar system formation, the survey of the asteroids, and others. Many missions have been organized to visit some planets of the solar system such as Mercury [1], Mars [2], and Jupiter [3]. Others have been targeted some asteroids, like Bennu [4] and Itokawa [5]. The planning of rendezvous with planets and asteroids still face many technical, theoretical, and economic problems. The near-earth rendezvous asteroids mission with a focus on the spacecraft designed is presented on the overview [6]. Some works have been interested by the autonomous rendezvous of the spacecraft with proximity operations [7]. The aspect of multi-rendezvous trajectory is shown

A. Anouar (✉) · M. Bennani
ENSAM RABAT, Mohammed V University, Rabat, Morocco
e-mail: anouaraziz.ing@gmail.com

M. Bennani
e-mail: m.bennani@um5r.ac.ma

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_5

in [8], as a design and optimization study. An interesting automatic rendezvous strategy between a passive vehicle and an active one orbiting around the earth-moon is considered in [9]. This paper focuses on the planning rendezvous for different planets of the solar system as well for the big asteroid Hygiea in the main belt of asteroid. A simulation synthesis is given to highlight the state of such planning strategies.

Finally, the conclusion is presented with some perspectives for the well exploration of the celestial objects in the solar system.

2 Formulation of the Rendezvous Problem

The problem of the rendezvous in interplanetary trajectories is how to launch some satellite (S) from planet (P_1) to reach planet (P_2). The chosen trajectory for this transfer is the Hohmann's elliptical orbit, as shown in the Fig. 1.

In the planning of the interplanetary rendezvous, we have to consider the outer configuration of P_2 relative to P_1 and the inner configuration $P_{2'}$ as shown in Fig. 2.

The relative angular position is given by

$$f = \Phi_0 + (\omega_2 - \omega_1)t \tag{1}$$

where

Φ_0 initial phase angle
ω_1 angular velocity of P_1
ω_2 angular velocity of P_2.

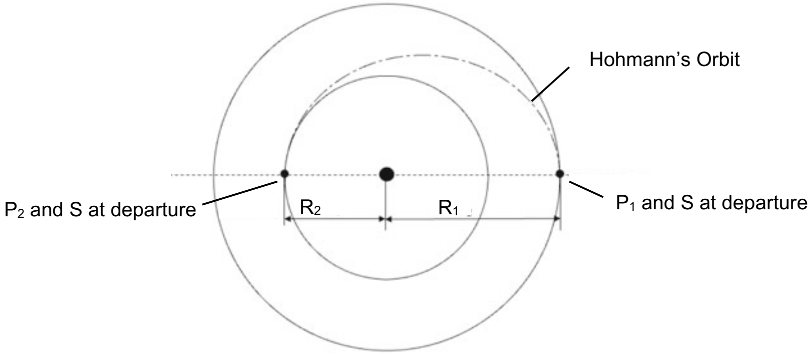


Fig. 1 Hahmann's transfer

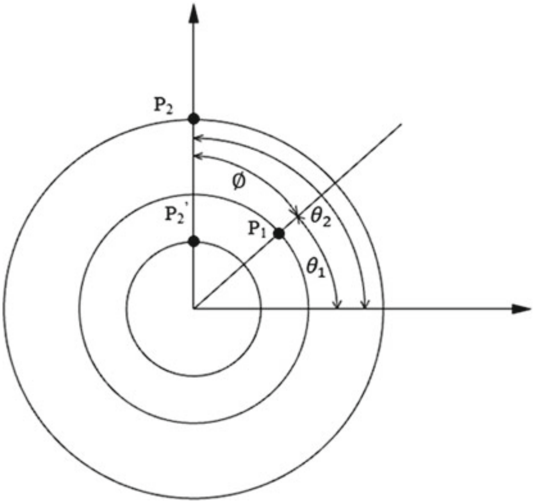


Fig. 2 Inner and outer configuration of P_2 relative to P_1

We can organize the interplanetary rendezvous in three phases, departure phase, where the satellite S is launched from a position attached to P_1 to reach some position of P_2 by following a semi-Hohmann's orbit in a time called t_h (Fig. 3).

t_h is the half of the period of the transfer ellipse with μ_s is the gravitational parameter of the sun defined as

$$t_h = \frac{\pi}{\sqrt{\mu s}}(R_1 + R_2)^{3/2} \tag{2}$$

$$\mu_s = M_s G \tag{3}$$

where M_s is the solar mass and G is the gravitational constant.

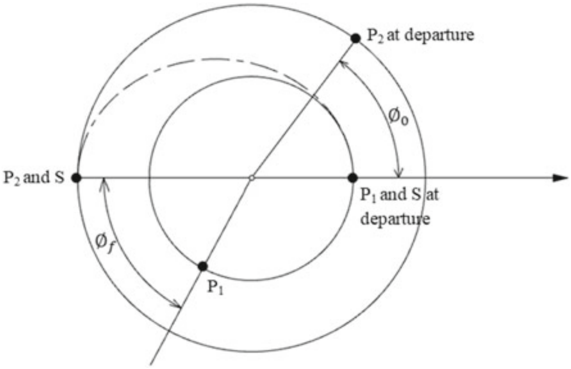
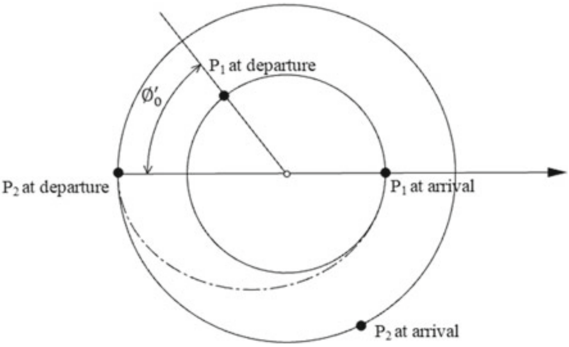


Fig. 3 Departure phase

Fig. 4 Waiting phase



Waiting phase: We have to prepare P_1 to be in good position to adopt the same semi-Hohmann orbit in the satellite return with the elapsed time t_h. Therefore, the new initial angle $\Phi_0^{'}$ is equal to Φ_f, and t_w is the required time for this phase (Fig. 4).

We can establish that

$$\Phi_f = \pi - \omega_1 t_w \tag{4}$$

And

$$t_w = \frac{-2\Phi_f - 2\pi k}{\omega_2 - \omega_1}((\omega_1 > \omega_2) \text{ for outer configuration})$$

$$t_w = \frac{-2\Phi_f + 2\pi k}{\omega_2 - \omega_1}((\omega_2 < \omega_1) \text{ for inner configuration})$$

k is an integer chosen to make t_w positive.

The meeting phase: We ensure the return of the satellite S attached to P_2 according to the semi-Hohmann orbit with the same time t_h to meet P_1 (See Fig. 3).

Thus, the global elapsed time t_g for the satellite in its trip is defined as

$$t_g = 2\,t_h + t_w \tag{5}$$

3 Simulation of Voyages in the Solar System

It is often useful for many interplanetary rendezvous to visualize the motion of the source planet, the target planet, and the satellite. So, we can implement all the concerning equations for the three main phases of the rendezvous in some simulation platform. Therefore, in this part, we are concerning of representing of the phases for the all the solar system planets and also for the Hygiea asteroid. The considered

Table 1 Considered data

Symbol	Name	Value
m_1	Mass of the sun	1989×10^{30} kg
G	Gravitational constant	6674.8×10^{-11} m^3 kg^{-1} s^{-2}
R_1	Distance Earth to sun	1 Au $\rightarrow$ 1496×10^9 m
R_2	Distance Mars to sun	1.52 Au
R_3	Distance Mercury to sun	0.39 Au
R_4	Distance Hygiea to sun	3.1415 Au
R_5	Distance Venus to sun	0.72 Au
R_6	Distance Jupiter to sun	5.2 Au
R_7	Distance Saturn to sun	9.54 Au
R_8	Distance Uranus to sun	19.2 Au
R_9	Distance Neptune to sun	30.06 Au
ω_I	Earth angular velocity around the sun	0.017202 rad/day
ω_2	Mars angular velocity around the sun	0.0091327 rad/day
ω_3	Mercury angular velocity around the sun	0.07139 rad/day
ω_4	Hygiea angular velocity around the sun	3.57×10^{-8} rad/day
ω_5	Venus angular velocity around the sun	0.028049 rad/day
ω_6	Jupiter angular velocity around the sun	0.001451 rad/day
ω_7	Saturn angular velocity around the sun	0.000593 rad/day
ω_8	Uranus angular velocity around the sun	0.0002049 rad/day
ω_9	Neptune angular velocity around the sun	0.0001044 rad/day

data are given in the Table 1. So as not to encumber the paper, we choose to put the graphs relative only to one inner configuration (Mercury), one outer configuration (Mars), and the asteroid. But the global results for the elapsed times are keeping in the simulation synthesis section.

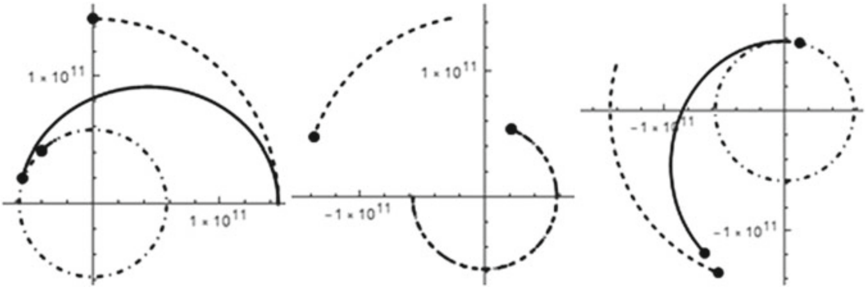


Fig. 5 Rendezvous with Mercury: **a** departure phase, **b** waiting phase, and **c** meeting phase

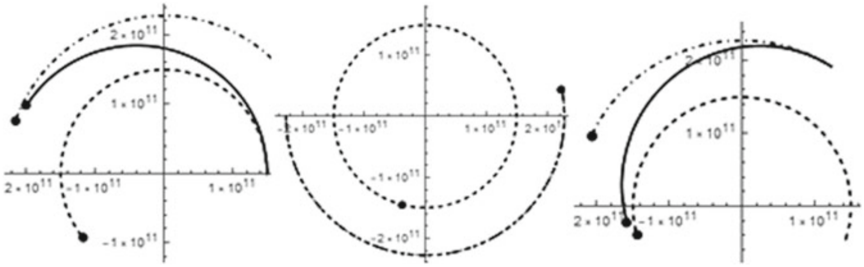


Fig. 6 Rendezvous with Mars: **a** departure phase, **b** waiting phase, and **c** meeting phase

3.1 Mercury Inner Configuration

The data of the rendezvous planning with Mercury are taking from the Table 1. The graphs concerning the departure phase, the waiting phase, and the return phase are given as in Fig. 5.

3.2 Mars Outer Configuration

For the planning of rendezvous with the planet Mars, we also consider its position relative to the sun and its rotational velocity from the Table 1. After simulation, we get the following graphs for the three phases (Fig. 6).

3.3 Asteroid Rendezvous

Many rendezvous missions have targeted asteroids like Bennu and Itokawa. We choose in this part to deal with the rendezvous planning with the asteroid Hygiea

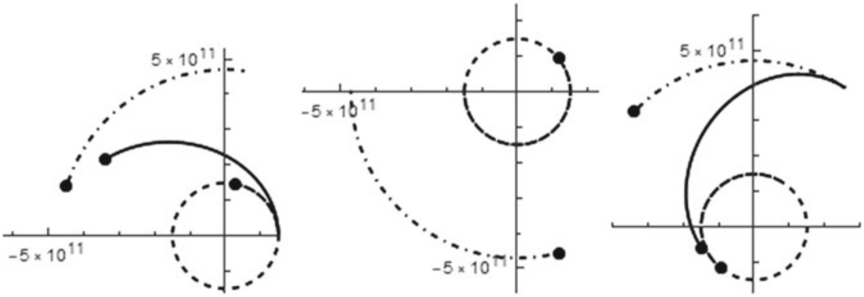


Fig. 7 Rendezvous with Hygiea: **a** departure phase, **b** waiting phase, and **c** meeting phase

(Table 1) which is one of the fourth largest asteroids in the asteroid belt. The simulation concerning the departure phase, the waiting phase, and the return phase are presented as in Fig. 7.

4 Simulation Synthesis

The elapsed times for the spatial trips of different planets and asteroid are presented in the Table 2 (Fig. 8).

The analysis of the above graph leads us to the following remarks:

- The departure time for the large planets is large than of the small ones. The variation of this time is nearly linear in function of the position of all the planets and asteroid relative to the sun (PAS).
- The ratio between the position of the rocky planets and the departure time is about one half. But it is increasing for the gas planets. It is also impressive to note that this ratio is nearly the same for Mercury and Uranus.

Table 2 Elapsed times of the spatial trips

	Departure time (years)	Waiting time (years)	Global time (years)
Mercury	0.297	0.178	0.739
Venus	0.390	1.249	2.03
Mars	0.709	1.243	2.66
Hygiea	1.49	3.68	6.66
Jupiter	2.73	0.586	6.05
Saturn	6.08	0.848	13.02
Uranus	15.67	0.688	32.03
Neptune	30.56	0.927	62.04

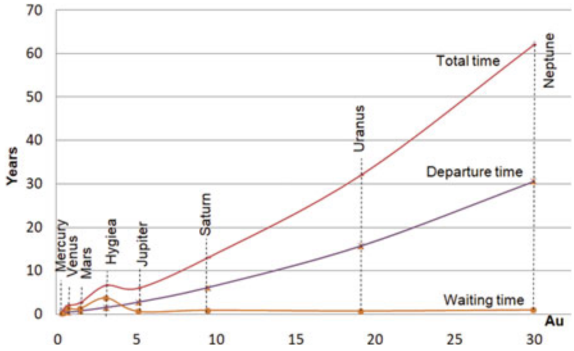


Fig. 8 Time graph of planet and asteroid

- The waiting time does not depend linearly of the positions of PAS as does the departure time. For Jupiter, this time seems to be the less relative to others. But the ratio of the waiting time with the position of PAS is too weak for the farthest planets such as Uranus and Neptune.
- The voyages to the farthest planets and their moons required more than ten year in simple trip. So we have to adopt other strategies for the trajectories planning like the assist gravity process and to enhance the propulsive techniques of the satellites.

5 Conclusion

We think more actually about the rendezvous planning missions with the planets and the asteroids of the solar system. The constraints are obviously expressed in terms of theoretical, technical, and economic aspects. This paper gives a clear sight to this rendezvous with different planets of the solar system and also with the big asteroid Hygiea located in the main belt of the asteroids. The well rendezvous formulation problem distinguishes the departure phase, the waiting phase, and the return phase. For each phase, the elapsed time is evaluated with a simulation of the orbits of the source planet, the satellite, and the target planet or the asteroid. Finally, the simulation synthesis helps to evaluate the rendezvous planning of these celestial objects of the solar system. It is also would be useful as a reference for other approaches such as the gravity assist and the trajectories optimization.

References

1. https://www.Planetary.org/space-missions//every-mercury-mission
2. https://mars.nasa.gov
3. https://www.nasa.gov/missions-pages/Jupiter/main/index.html
4. https://www.Nasa.gov/Osiris-rex

5. https://www.Nature.com/articles/5541598-021-24517-x
6. John Hopkins University applied laboratory: Near earth asteroid rendezvous spacecraft overview. In: Proceeding IEEE aerospace applications conference (1996)
7. Lu P, Liu X (2013) Autonomous trajectory planning for rendezvous and proximity operations by conic optimization. J Guidance Control Dyn 36(2):375–389
8. Federici L, Zavoli A, Colasurdo G (2019) Impulse multi-rendezvous trajectory design and optimization. In: 8th European conference for aeronautics and space science, Madrid, Spain, July 2019
9. Buccioni G, Innocenti M (2021) Rendezvous in Cis-Lunar space near rectilinear halo orbit: dynamic and control issues. J Aerosp 8:68

Peak Shaving in Microgrids Using Hybrid Storage

Juraj Londák, Radoslav Vargic, and Pavol Podhradský

Abstract In this contribution, we focus on technical and economic aspects of using hybrid storage in microgrids for peak shaving. We perform feasibility analysis of hybrid storage consisting of conventional supercapacitors and chemical batteries. We use multiple real-life consumption profiles from various industry-oriented microgrids. The primary purpose is to construct digital twin model for reserved capacity simulation and prediction. The main objective is to find the equilibrium between technical innovations, acquisition costs, and energy cost savings.

Keywords Microgrid · Peak shaving · Energy storage · Digital twin

1 Introduction

Recent development in electric energy sector includes strong demand for distributed means to help to maintain the electricity network in good condition. As well as the motivation of the consumers is to minimize the bills with regards to reserved capacity. One of such means what can help in both cases is peak shaving.

For most customers, energy consumption changes through the workday, with significant peaks and valleys. To accommodate this variable demand at the grid level, utility providers may also vary their pricing throughout the day [1]. Peak shaving methods [2] generally refer to leveling out peak usage of energy by whole spectrum of energy consumers. The main purpose of peak shaving from customer point of view is to save on the electricity bill [3]. Grid operator on the other hand can benefit from peak shaving by more stable and balanced network and consumption. Understanding the risks of peak shaving, we need to start with understanding how is the electricity billed by Slovak grid operators. The data collected by distribution company contain information of how much electricity customer consumed (kWh) and the peak load (kW). The network provider charges customers a sum of money for each kW of reserved Ccapacity during accounted period. Customer should typically decide

J. Londák (✉) · R. Vargic · P. Podhradský
Faculty of Electrical Engineering and Information Technology, STU, 812 19 Bratislava, Slovakia
e-mail: juraj.londak@stuba.sk

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_6

upfront on capacity he expect to demand for certain fixation period. Peak shaving with help of various energy storage systems allows customer to postpone or balance this expected peak consumption. It can have significant positive consequences on billed reserved capacity.

Recently, the electric energy storage sector is in huge development driven mainly by environmental motivations. Energy storage plays crucial role in the peak shaving process. We review this part in Sect. 2.

To be able to simulate the technical–economic aspect, one of the approaches is to construct digital twin. The digital twin is reviewed in the Sect. 3. Following the digital twin approach, we constructed own simulation environment based on the MATLAB. We introduce the created environment in the Sect. 4. The results for selected use cases with regard to peak shaving and hybrid battery storage are described in the Sect. 5.

2 Energy Storage Systems

Electrical energy storage (EES) is a method of transforming electric energy from source or network into a storable form and back when needed. It allows electricity to be produced when it is cheap to generate or from unpredicted energy source. It can be then used when there is higher demand for energy or when it is not available.

The traditional electricity grids are built for the simple one-way transport from source to consumer. This traditional concept presumes electricity consumption is coupled with production. However, electricity consumption changes significantly during days, weeks, and months, the maximum consumption typically last only short time during each month or even year. This leads to ineffective and expensive power plants and distribution networks. Storage systems allow energy production to be decoupled from generation.

EES has many applications including portable devices, vehicles, and fixed energy resources [4].

In Sect. 2.2, we have worked with hybrid battery concept, which combines both energy management and UPS functions. We have merged conventional chemical battery suitable for energy management function with higher energy capacity and high-power rating supercapacitor for power quality function. This combination covers both contradictory functions stated above.

2.1 Conventional Monomode EES

Rechargeable battery is one form of electricity storage [4, 6] which stores electricity in the form of chemical energy. Electrochemical reactions during discharge process occur at both electrodes creating a flow of electric energy through an connected circuit. This process is reversible which allows battery to be recharged by connecting

Table 1 Characteristics of selected types of storage systems [6]

Systems	Power rating and discharge time		Storage duration		Capital cost	
	Power rating	Discharge time	Self-discharge per day (%)	Suitable storage duration	$/kW	$/kWh
Chemical batteries	0–20 MW	Seconds-hours	0.1–0.6	Minutes-days	300–4000	200–2500
Capacitor	0–50 kW	Milliseconds – 60 min	40	Seconds–hours	200–400	500–1000
Supercapacitor	0–300 kW	Milliseconds – 60 min	20–40	Seconds–hours	100–300	300–2000

to power source to the battery. We have summarized typical characteristics of both used storage systems in Table 1.

2.2 Supercapacitor

Capacitor is the most direct mean how to store electric energy. They are able to charge significantly faster than conventional batteries and can be used for much higher cycles with a better efficiency. Conventional capacitors are suitable for daily peak loads under 1 h because of their small capacities—the main drawback of capacitors is their relative low-energy density.

Current progress in the supercapacitor development could lead to much greater capacitance and energy density. Supercapacitors have much higher storage capabilities in comparison with conventional capacitors (10–100 s kW) [5]. The main difficulty using capacitors is related with short discharge intervals and high self-discharge energy loss when not in used.

2.3 Hybrid Batteries

Hybrid power source combines multiple sources of energy with distinctive characteristics. Hybrid power sources combining different variations of fuel cell, battery, and supercapacitor are popular in automotive systems [7, 8].

Hybrid battery-supercapacitor power sources can merge together individual benefits of batteries and supercapacitors. Batteries provide high capacity, low-peak power, long charge times but also low self-discharge, and relatively low watt-hour costs. On the opposite, the supercapacitors have small energy capacity, higher peak power, short charge times with high self-discharge, and high watt-hour costs [9].

Further, in the paper, we perform multiple simulations using simulator described in Sect. 4 of this paper. Battery consisting of multiple sources raises question about order of charging and discharging of segments itself. Different strategies cause different effectivity in real-life environment and have implications battery life cycle.

As we have stated earlier, we chose chemical battery in combination with supercapacitor as our combination. We have implemented typical characteristics (see Table 1) of both types to simulation environment [10] as we have created digital twin of both physical batteries.

3 Digital Twin in Energy Sector

Current trend in utility sector with complex distributed power sources, energy storage systems, prosumers, and microgrids creates difficult ecosystem to manage and even control. This raising complexity generates need for virtual representation of physical reality to accelerate predictability of such complex systems. Concept of digital twin comes handy here, where universities and utility providers create digital twins of selected parts of their infrastructure [11, 12].

A digital twin concept is a virtual representation that serves as the real-time digital counterpart of a physical object or process. The concept and model of the digital twin were publicly introduced by Grieves [13]. Grieves proposed the digital twin as the conceptual model underlying product lifecycle management (PLM).

The concept of the digital twin predates the Industry 4.0 era as well as the digital age itself. Its roots go back to the 1970s, when NASA worked on the Apollo project. During the Apollo 13 mission, an oxygen tank exploded, seriously damaging the service module, and endangering not only the mission itself, but especially the lives of the entire crew on board. Because they had a exact replica of the spaceship on earth with all the technical details, they could reliably simulate a dangerous situation and realistically test hypothetical solutions.

The same principle applies to production and logistics processes, traditional technologies, and methods have already become insufficient to ensure sustainable growth. This means that they can no longer meet the new requirements of the industry—from cost optimization to consumer customizations in mass production.

Creating models of real machines in operation allow industrial companies use additional data and algorithms to make better decisions. Obtained data can be used for improving processes, reducing costs, and improving customer experience.

A demo platform for virtual power plants implementing digital twin concept is maintained at Reutlingen University [14, 15]. It is used for the study of different methods of operation, optimization, and control of grids and distributed energy devices [16].

At present, the term digital twin means a virtual representation of objects and entities such as manufacturing and transport equipment, but also processes, systems, workers, data, or the whole environment. These days, the digital twin has moved from plain virtual model of the physical product to a dynamic carrier of data and status information obtained through several sensors connected by the Internet of things (IoT).

Their use in complex simulation models speeds up and simplifies decision-making processes, as it simplifies the direct identification of the possible consequences of the considered changes as well as the key patterns of behavior in individual processes.

The digital twin in this form is therefore used to monitor entities as well as processes in real, as this technology allows to create a very detailed digital image with real data.

4 Simulation Environment

For the purpose of the techno-economic analyzes and with conformance with the digital twin concept, we developed a new smart grid simulator for techno-economic analysis (SGSTEA). The simulator is built in MATLAB environment and strongly uses object-oriented programming. It does not use Simulink nor Simscape electrical. The system is provided as open source along with demos and demo data [10]. The systems lacks own GUI and offer set of specific classes and demo classes that can be used to build complex techno-economic scenarios. The basic difference against Simscape electrical is that we do not aim to build electrical network but energy generation, storage, transportation, consumption network with 15 min basic tact and with strong economic aspect. So the objects such as batteries besides the technical parameters have APSO economic parameters such as OPEX and CAPEX including deprecation modeling.

The system implements the most important elements and concepts of smart grid technologies and hybrid battery technology. Especially, the SGSTEA environment can be used to predict the suitability of connecting different types of batteries used for "peak shaving" [17] or "load leveling." The output of such a simulation is not only technical information about the power network but also the expected economic profitability for participating roles and return in the form of return of investments (RoI) computations. The basic concept of the techno-economic simulations is

(1) first run the technical simulation in the "imulation time" (e.g., one month, one year, … in precise 15 min steps) and measure behavior of the components and modules and whole microgrid
(2) second, based on "simulation time" results, run extended economical analysis is "economic time" that can extrapolate the results (typically to 15 years) and concentrate on economic aspects such as RoI and profitability for the participating roles

Of course, this basic concept includes several extensions for iteration, searching for optimum, updating the model parameters, etc. Basic conceptual architecture is shown on Fig. 1. Here, you can see the basic types of modules and data flows between them. The basic level of smart grid controls and helps to optimize the single location that can be connected to the electricity network. This (based on

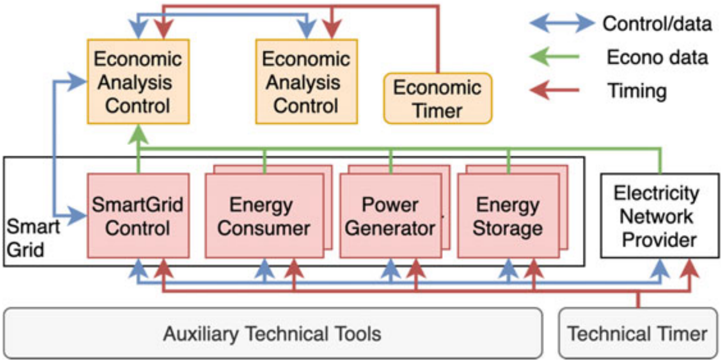


Fig. 1 Basic concept of the SGSTEA simulator, depicted are basic types of modules and data flows

legislative) could correspond to single prosumer (provider + consumer). Prosumers can be stacked, i.e., used instead of consumer block on Fig. 1, so the simulation can be multilevel and providing the situation view, e.g., for local or regional electricity distribution operators. The basic types of modules are and can be further split into more specialized types of objects, such as energy storage to battery or other type of storage, batteries to further subtypes as described in the Sect. 2. Due to the object-oriented nature of the simulator it can be easily extended with more specific modules. More detailed information and documentation can be found in [10].

5 Simulation Results

We performed multiple simulations in the previous paper [11] to determine optimal battery capacity and power for best peak shaving performance and RoI ratio in multiple real-time scenarios. In this paper, we present analysis of further various topics related to peak shaving using the provided simulation environment, focusing on energy storage, and reserved capacity topics.

5.1 Scenario1—Comparison of Hybrid Energy Storage Algorithms

To analyze the potential and main artifacts of hybrid battery storage related to charging and discharging, we constructed the hybrid battery with slow part (chemical battery) and fast part (supercapacitor)—with typical parameters according to Table 2. With relation to charge/discharge order, we have 4 basic algorithms. E.g., fast battery is charged first and slow battery after, only in case if (real/forecasted) power/energetic

Table 2 Charge/discharge strategies for all algorithms

Algorithm number	Charge order	Discharge order
Algorithm 1	Fast, slow	Fast, slow
Algorithm 2	Fast, slow	Slow, fast
Algorithm 3	Slow, fast	Slow, fast
Algorithm 4	Slow, fast	Fast, slow

balance allows it, fast battery is discharged first, then slow, only in case that energy from fast battery is not sufficient. This is denoted as Algorithm 1. Table 2 sums up all possible algorithms. Of course, there if full span of options "between" that the energy is split while charging, e.g., 30–70% between battery parts. In this scenario, we examined the border cases.

The input to the hybrid energy storage is power requesting/offering signal, where positive values mean offering the power to storage, negative values mean requesting power from the storage. Output signal gives information about stored energy (positive values) or offered energy (negative values). To be able to evaluate the situation, we constructed the input power demanding/offering signal as superposition of two periodic signals.

First one is with fast changes, zero mean—easy to peak shave with standalone fast battery. Second one is with slower changes, but with negative mean (i.e., in each cycle, slightly more energy is demanded as offered), easy to shave with slow battery, but only until full discharge is reached. So, the fully charged batteries at the start of the simulation get discharged for sure during the simulation, but we can observe the accompanying artifacts during the simulation. In our simulation, the winning algorithm is Algorithm 1. The details for all algorithms are in Figs. 2 and 3. In Algorithm 1, the fast battery is fully used, and it fails as expected due

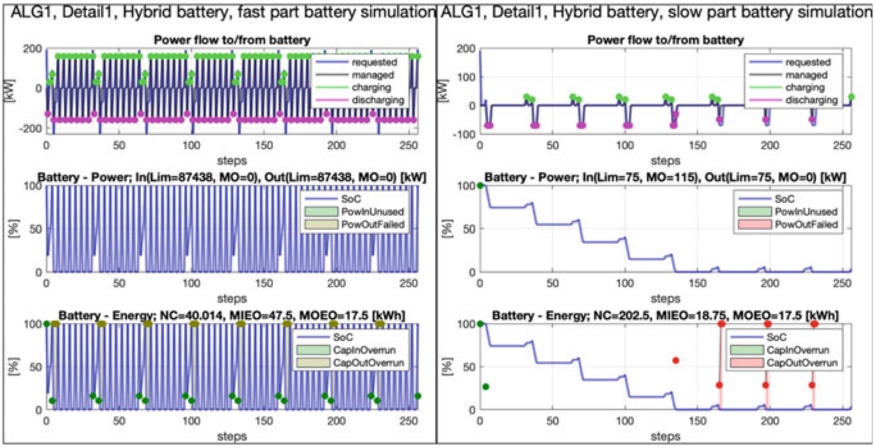


Fig. 2 Hybrid battery scenario, winning Algorithm 1 performance, battery fails to deliver the power due full discharge of slow battery in step 135 (first red dot in the right bottom graph)

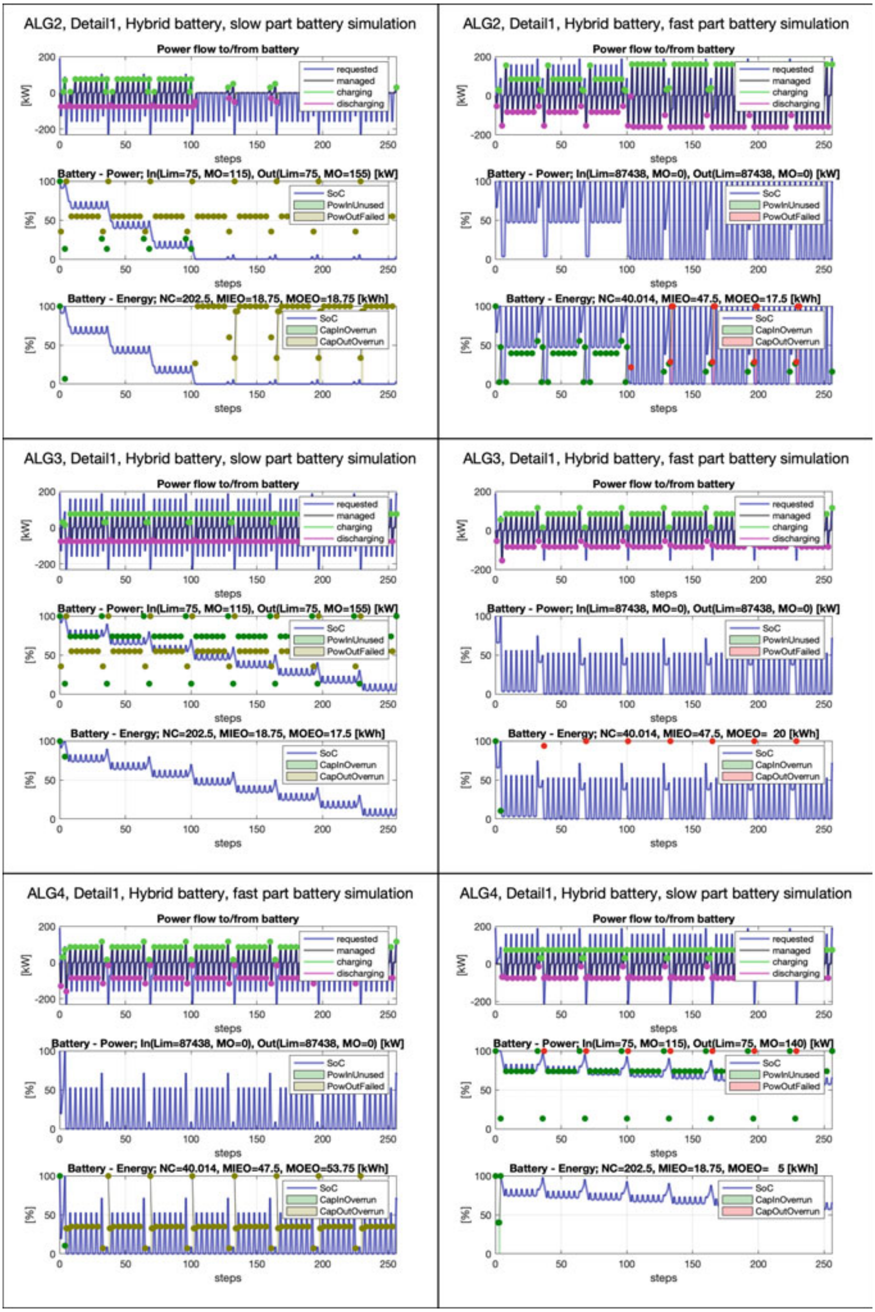


Fig. 3 Hybrid battery scenario1, sooner power/energy delivery failures of the second battery while discharging (red dots) when using the Algorithm 2, 3, 4 in the hybrid battery. Algorithms 2 and 3 fail due full discharge of the second (fast) battery, algorithm fails due problem to deliver requested power from the slow battery while fast was fully discharged

to negative balance of the input signal. In Algorithm 2, the slow battery goes fully discharged significantly faster as the fast battery is preferred in charging, resulting into immediate problem due to fast battery capacity. In Algorithms 3 and 4, the charging prioritization in charging causes imbalance—though the slow battery is richly charged, we are unable to get the sufficient energy in time—the faster battery gets fully discharged quickly, and slow battery is unable to deliver the needed power.

5.2 Scenario 2—Fines Increase upon Initial RC Decrease

To exploit the potential of hybrid battery usage in microgrid, we propose to simulate the microgrid for initial RC decrease with specified battery size. The simplified border cases are, that the battery is 100% slow (bad parameters but cheap) or 100% fast (good parameters but expensive). As the RC decreases, the battery is needed more and more. From certain instant, the RC increase is necessary to be able to fulfill the consumption needs. The situation example for different battery sizes is shown in Fig. 4. We can see that for given profile, the difference between slow and fast is relatively small and significant only for smaller battery cases, so the eventual RoI shall be interpreted with caution. More surprising observation is presence of big jumps in the fines, clearly decrease of reserved capacity can cause also significant decrease of fines. The simulation environment can give clear explanation for this as depicted on Fig. 5. In the upper set of graphs is microgrid A with initial RC = 1013 kWh and RC increase up to 1075 kWh in simulation steps 911–918. In lower set

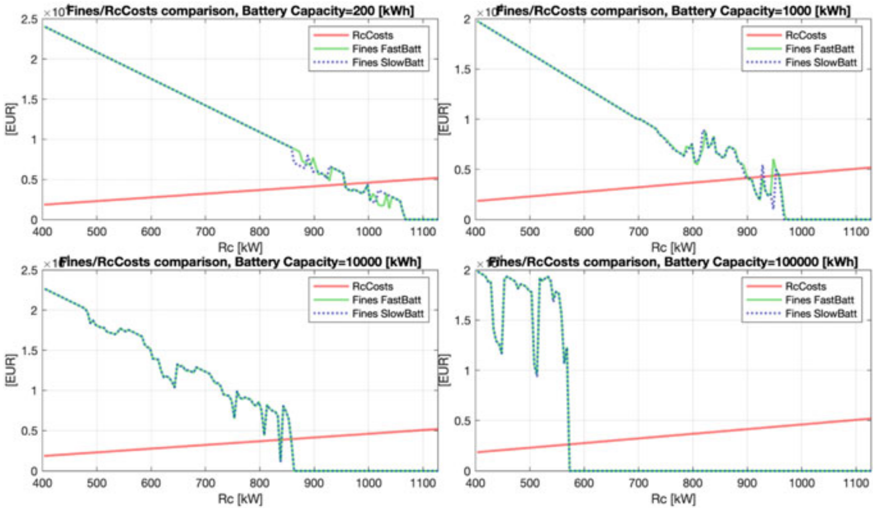


Fig. 4 Scenario 2 example, initial RC decrease causing increase of fines, evaluation of border cases of hybrid battery composition for selected battery sizes

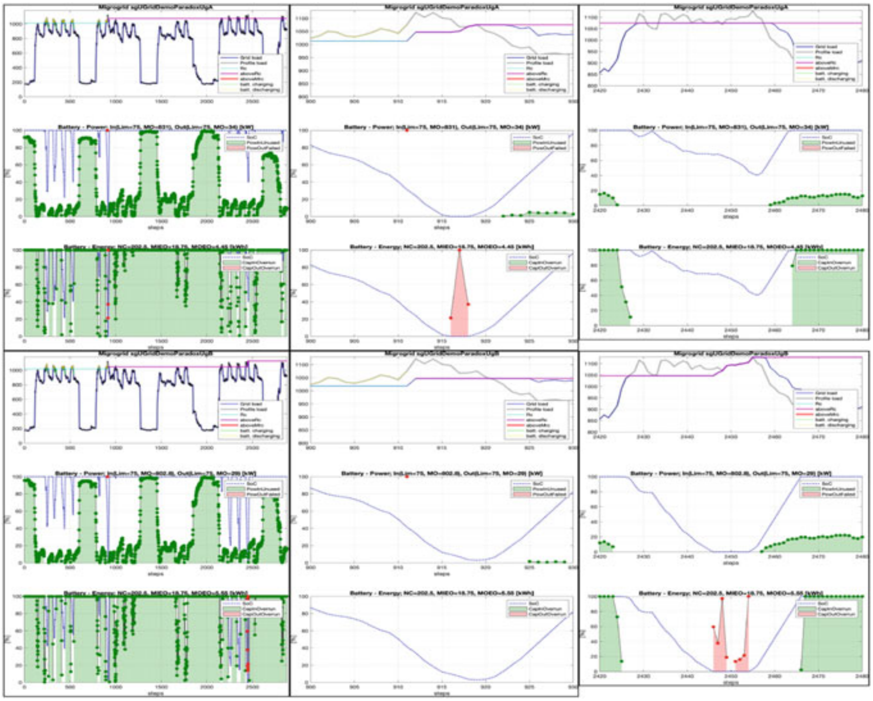


Fig. 5 Scenario 2, example, explanation of paradox, whereby decreasing the initial reserved capacity can cause significant decrease of fines

of graphs—Microgrid B with initial RC = 1018 and smaller RC increase to 1047 kWh in steps 911–918 but with additional significant increase up to 1128 in steps 2446–2454. So the reason is that we could have better situation most of the time, but if accidently the battery power runs out at the wrong time, it can cause much more economic damage. The effective solution for this situation could be to progressively increase the RC value sooner (based on the consumption statistics) and not to wait until the battery is discharged. So this topic is subject for optimization in microgrids.

6 Conclusion

We have presented our contribution to digital twin implementation in utility sector in this paper. Presented simulator [14] can serve for simulation, optimalization, and prediction purposes. We have shown interesting scenarios related to peak shaving and costs related to reserved capacity. Presented contribution will also serve as teaching aid for academic purposes and will be transferred to academic projects DiT4LL and KEGA project MonEd as pedagogical research. Presented simulator is prepared for future extensions as open-source project. One of the most interesting extensions is photovoltaic functionality.

Acknowledgements This publication was created thanks to support under the Operational Program Integrated Infrastructure for the project: International Center of Excellence for Research on Intelligent and Secure Information and Communication Technologies and Systems—II. stage, ITMS code: 313021W404, co-financed by the European Regional Development Fund

References

1. Oudalov A, Cherkaoui R, Beguin A (2007) Sizing and optimal operation of battery energy storage system for peak shaving application. IEEE Lausanne Power Tech 2007:621–625. https://doi.org/10.1109/PCT.2007.4538388
2. Moslem U, Fakhizan RM, Faris AM, Syahirah AH, Bakar A, Halim A, Tan ChK (2018) A review on peak load shaving strategies. Renew Sustain Energy Rev 82(P3):3323–3332
3. Ahcin P, Berg K, Petersen I (2019) Techno-economic analyis of battery storage for peak shaving and frequency containment reserve, pp 1–5. https://doi.org/10.1109/EEM.2019.8916380
4. Mclarnon FR, Cairns EJ (1989) Energy storage. Ann Rev Energy 14:241–271
5. Chen H, Cong TN, Yang W, Tan C, Li Y, Ding Y (2009) Progress in electrical energy storage system: a critical review. Progr Nat Sci 19(3):291–312. ISSN 1002-0071
6. Baker JN, Collinson A (1999) Electrical energy storage at the turn of the millennium. Power Eng J 6:107–112
7. Chai R, Ying H, Zhang Y (2017) Supercapacitor charge redistribution analysis for power management of wireless sensor networks. Power Electron IET 10(2):169–177
8. Bayhan S, Abu-Rub H, Ellabban O (2016) Sensorless model predictive control scheme of wind-driven doubly fed induction generator in dc microgrid. Renew Power Gener IET 10(4):514–521
9. Baumann M, Buchholz M, Dietmayer K (2017) Model predictive control of a hybrid energy storage system using load prediction. In: 2017 13th IEEE international conference on control & automation (ICCA), pp 636–641
10. Vargic R (2021) sgstea (https://github.com/radovargic/sgstea/releases/tag/v1.1), GitHub. Retrieved 25 Aug 2021
11. Tugarinov P, Truckenmüller F and Nold B (2019) Digital twin of distributed energy devices. In: Proceedings of the international scientific and technical conference: forum of mining engineers. NTU Dnipro Polytechnic Press, pp 323–331
12. Zhang ZJ, Nair NC, Cross S (2015) Modeling and simulation framework for techno-economic analysis of large city low-voltage distribution network. IEEE Innov Smart Grid Technol Asia (ISGT ASIA) 2015:1–6. https://doi.org/10.1109/ISGT-Asia.2015.7387052
13. Grieves M (2019) Virtually intelligent product systems: digital and physical twins. In: Flumerfelt S (eds) Complex Systems engineering: theory and practice. American Institute of Aeronautics and Astronautics, pp 175–200.
14. P. Tugarinov, F. Truckenmüller and B. Nold, "Virtual Power Plant Demonstration Platform," Forum of Mining Engineers, Dniepro, 2019.
15. Reutlinger Energiezentrum, Virtuelles Kraftwerk Neckar-Alb, 22 July 2019. [Online]. Available: http://www.virtuelles-kraftwerk-neckaralb.de/demonstrator/
16. Heimgärtner F, Schur E, Truckenmüller F, Menth M (2017) A virtual power plant demonstration platform for multiple optimization an control systems. In: International ETG congress, Bonn, Germany
17. Londak, Vargic J, Podhradský R (2021) P-peak shaving in microgrids using battery storage. In: IWSSIP 2021, Proceedings in progress, June 2021

A Machine Learning Approach to Predict SEER Cancer

Dm. Mehedi Hasan Abid, Tariqul Islam, Zahura Zaman, Fahim Yusuf, Md. Assaduzzaman, Syed Akhter Hossain, and Md. Ismail Jabiullah

Abstract The SEER database is among the persuading stores regarding malignancy pointers inside us. The SEER list helps impact investigation for the gigantic measure of patients' bolstered viewpoints for the most part ordered as an insightful segment and impact. Assistant careful proof nearly the carcinoma dataset is ordinarily started on the site of the National Cancer Institute. The main point of this work is that depending on the individual's manifestations, and we will foresee whether individuals are in danger of malignant growth or not. Perseverance and desire for the benefit of malignant growth patients have the option to upsurge prophetic exactitude and limit in the end cause better-educated decisions. To the current end, various amendments smear AI to disease data of the surveillance, epidemiology, and end results database. It may be used to better forecast cancer in the medical sector, and these studies can give a good chance to enhance existing models and build new models for uncommon cancers of minority groups in particular. In this paper, the authors contribute to getting more predicted accuracy for SEER cancer and use it to better forecast cancer in the medical sector.

Dm. M. H. Abid (✉) · T. Islam · Z. Zaman · F. Yusuf · Md. Assaduzzaman · S. A. Hossain · Md. I. Jabiullah
Daffodil International University, Dhaka, Bangladesh
e-mail: mehedi15-226@diu.edu.bd

T. Islam
e-mail: tariqul15-2250@diu.edu.bd

Z. Zaman
e-mail: zahura15-1381@diu.edu.bd

F. Yusuf
e-mail: fahim15-2239@diu.edu.bd

Md. Assaduzzaman
e-mail: assaduzzaman.cse@diu.edu.bd

S. A. Hossain
e-mail: akhter.hossain@ulab.edu.bd

Md. I. Jabiullah
e-mail: drismail.cse@diu.edu.bd

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_7

Keywords SEER cancer · Carcinoma · Epidemiology · Machine learning · Data mining

1 Introduction

SEER is an authoritative source for cancer surveillance, epidemiology, and end results. The SEER program gives information about cancer statistics that stick up for efforts to reduce the cancer compulsion within the people. The main point of this paper is that depending on select manifestations, and we will foreknow whether individuals are at threat of malignant growth or not. In the dataset the scope of straight capacities leveling as 0 and 1. The outcome will give the likelihood of being threatening as 1 and amiable as 0. Possibly, the most famous supervised learning computations, which is used to categorize, are the support vector machine. It is mostly used in machine learning (ML) classifications. The goal of the SVM computation is to establish the optimal line or choice limit which can be used to isolate n-dimensional room in classes so that we can without uncertainty classify the fresh information point later. SVM picks definitive focuses or vectors that help in making the hyperplane. For arrangement and relapse examination, SVM perceives designs and dissects the information. To acquire better execution in SVM, Kernel capacities have been applied. Notwithstanding, the train test level of information is 70% and 30%. The decision tree calculation is one of the most straightforward yet solid supervised machine learning calculations. The decision tree calculation can be utilized to tackle both relapse and arrangement issues in machine learning. That is the reason, it is otherwise called CART or classification and regression trees. “The method of choosing trees to tackle an issue is tree portrayal. J48 form is applied in this paper for building the choice tree. Entropy and information gain are utilized to build the tree. The segment of train and test information is 70% and 30%. This work is the proposed upper three algorithm acknowledgment of machine learning technique for analysis disease and predicts better accuracy” [1]. Perseverance and desire for the benefit of malignant growth patients have the option to upsurge prophetic exactitude and limit in the end cause better-educated decisions.

2 Related Work

The office to evaluate carcinoma life expectancy bolstered disorder qualities since antiquated patient masses could even be helpful while examining exact patients and may thus help current clinical practice [2]. “Data out of BDHS, 2014 is used, factors like arithmetical, more economic, and natural have a differential influence on abate. The DT algorithm was enforced to find the aspect combined with stunting. It is found that mothers’ education, birth order number, and economic status were associated with stunting. Support vector machine and artificial neural network are also enforced with the stunting dataset to test the accuracy. The certainty of the decision tree is 74%, SVM is 76%, and ANN is 73%" [2]. Extra work has assessed life expectancy rates for rectal and restricted stage little cell malignant growth. Expectation models for life expectancy time or a choice of different components are investigated normally [3]. These endeavors have included managed AI characterization systems, preparing, and measurements. As far as ML, directed learning calculations arrange records with named information [4–6]. The capacities surmised from the named preparing information would then be able to be wont to group new information. Interestingly, solo methods do not utilize named information; the strategy is predicated on estimating the similitude of intra classes and divergence of "bury" examples while limiting the earlier suspicions [7, 8]. This procedure yields a "backwoods" of arbitrarily created choice trees whose results are incorporated as a "group" by the calculation to foresee more precisely than one tree would. As thought about, gradient boosting machine (GBM) utilizes more vulnerable, littler models to make a "troupe" to supply the last expectation. New powerless models are iteratively prepared concerning this entire outfit [9, 10]. Support vector machines (SVMs) are a case of non-probabilistic double rectilinear relapse [11–13]. Here, we investigate the capability of unaided AI strategies for carcinoma persistent endurance expectation [14]. These strategies intrinsically include less human ability and connection than regulated techniques and in this way, limit required intercession for database examination [15]. Longer-term, the mechanized order of patients into gatherings may encourage correlation and assessment of prognostic likewise as demonstrative contemplations in clinical practice. Malignancy is the second driving clarification for death inside the earth [16]. The premier regular sorts are bosom and carcinoma with 268,670 and 234,030 anticipated new cases in 2019. Applying AI for endurance expectation, for example, foreseeing whether a patient having malignancy after determination can build the prognostic precision and may at last reason better-educated choice [17]. The NCI gathers disease rate and endurance data covering over 30% of the populace inside the U.S. because of its wide inclusion and exhaustive information assortment, SEER information could likewise be a reason for a few endurances forecasts exploring different avenues regarding AI [18]. On the off chance that a direct partition is unimaginable, the strategy applies piece techniques to perform non-straight mapping to an element space, during which the hyperplane speaks to a non-direct choice limit inside the information space [19, 20]. In the paper, Snow et al. [21] proposes that breast cancer has a risk of developing RIS compared to other solid cancers.

3 Proposed Method

In this application, the admissible report is closely knit from the NCI [22]. Data collected from the analysis performed in appropriate studies are only a couple of research areas currently supported by the SRP. The proposed research methodology and the flow of operations are depicted in Fig. 1.

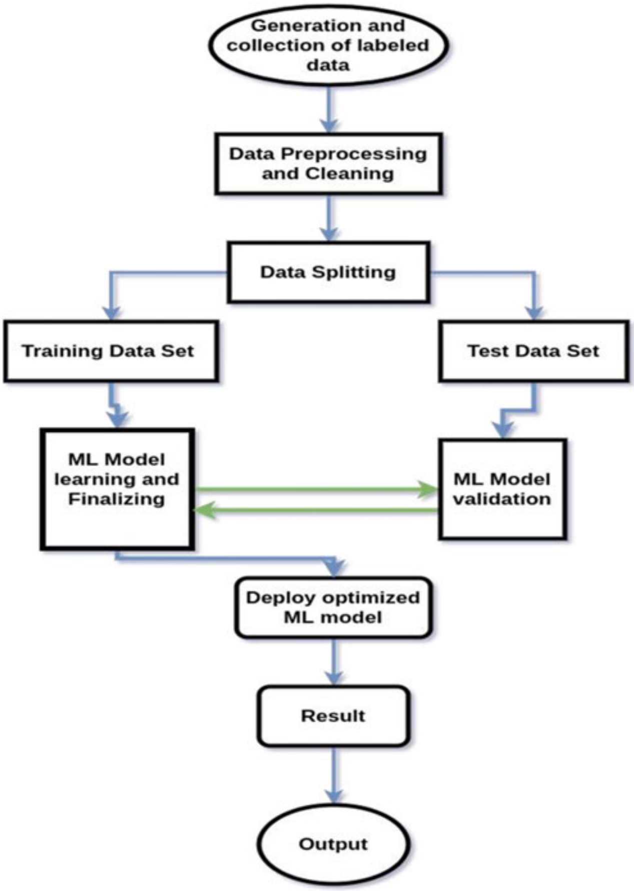

Generation and collection of labeled data
Data Preprocessing and Cleaning
Data Splitting
Training Data Set
Test Data Set
ML Model learning and Finalizing
ML Model validation
Deploy optimized ML model
Result
Output

Fig. 1 Flowchart of the proposed engaged development

First of all, since the datasets [22] were in multiple files, we gathered data from the National Cancer Institute, and then merged the data. Next, we optimized the SPSS datasets and separated the information sets. After that, for each dataset, we trace the Z-score. Next, we equate the score to the diagnostic status of the cheque. Finally, to implement different algorithms such as decision tree, help vector machine, and artificial neural network algorithm, we allow testing datasets (70%) and evaluation datasets (30%). This study brief offers three benefits of developed and popular diagnostic procedures.

3.1 Label Encoding

The label encoding is done when the dataset contains categorical values. Turn absolute values into numerical values by replacing data categories with integers starting with 0. No need to do the previous operations. To convert this into numerical values, the authors will use the “LabelEncoder” class from scikit learn. Labels have been replaced with integers.

3.2 Accuracy Rule for ANN, SVM, and DT

The confusion matrix is used for interpret the classification model representation. There are also four potential results for “TN = true negative, FN = false negatives, FP = false positives, and TR = true positive” in the confusion matrix for two-class cases: one is 0 and another 1. The evaluation of a classifier, as described by, is usually assessed in several performance tests such as precision, sensitivity,

$$\text{Accuracy} = \text{TP} + \text{TN}/(\text{TP} + \text{TN} + \text{FP} + \text{FN}) \tag{1}$$

$$\text{Sensitivity} = \text{TP}/(\text{TP} + \text{FN}) \tag{2}$$

The proportion of instances evaluates accuracy. Sensitivity measures a percentage of negative cases.

4 Data Preparation and Data Source

NCI gathers information on malignant growth cases from different areas and sources all through the United States. Information assortment started in 1973 with a set number of libraries and keeps on extending to incorporate significantly more zones and socioeconomics, countrywide example overviews of people of generative age created to give data on malignancy and different levels. The essential key factors in our datasets are sweep, surface, border territory, perfection, conservativeness, concavity, inward focuses, balance, and fractal measurement. There are 570 datasets with medium, standard error dividers, and the most notable of these highlights are shown, with around 30 highlights for each picture. The mean radius is field 3, radius SE is field 13, and the worst radius is field 23, for instance [22]. To apply a calculation, the information was not prepared. Right off the bat, the information was in a few divisions such as mean, SE, worst. At that point, we blend the information records utilizing the SPSS instrument. However, an enormous amount of information was missing in the informational index, which is the reason nonappearance information was dealt with by the separating interaction. Ultimately, the information examined to look out the measurements in proportion to get how much individuals are tormented from determination.

5 Experimental Results

Diagnosis is a proportion of the relevant examples collected over the entire number of cases. Accordingly, the accuracy and the radius in this table are based on an understanding and standard of three algorithms. The confusion matrix of ANN, SVM, and DT algorithms with the label, precision, recall F1-score, and support values is presented in a tabular form in Table 1.

From 570-column information, 60.82% precision and 99% review is NO, where 75% exactness 4% review is YES for ANN. Another calculation gives 60% exactness and 100% review is NO, where 100% accuracy 3% review is YES for SVM. Ultimately, DT precision is 95% and 97% exactness and 97% review is NO, where 95% accuracy 93% review is YES.

The DT method has the best accuracy and execution rate among the various algorithms studied. The study also shows that the optimal parameter values for penalty. Parameter and pyramid levels can improve the classification result. The overall accuracy of the SVM and ANN is low because the main variable used are “radius_mean, texture_mean, perimeter_mean, area_mean, smoothness_meanconcavity_mean, concave points_mean, symmetry_mean and fractal_dimension_mean.” Therefore, the value variable was also used to separate. The study also shows that mean and value variables are suitable to be used in DT classifier. We partition the dataset into isolated segments like the preparation dataset is 70% and for testing, it is 30%. But SVM, precision and recall give 100% for its kernel trick to handle nonlinear input spaces. SVM finds an optimal hyperplane which helps in classifying new data points. In the time of training, SVM gained the knowledge about that data, and now if you give same data to predict, it will give exactly same value. This work is the proposed store-up AI method for examination illness, in which we can discover in the table and figures that the proposed methodology is showing up with 100% precision. At this moment, only 32 feature for the assurance of sickness. Later on, all features of UCI are tried and achieved with the best accuracy. Using random forest returns a

Table 1 Confusion matrix of ANN, SVM, and DT

Algorithms	Label	Precision	Recall	F1-Score	Support
ANN	No	0.60	0.99	0.75	102
	Yes	0.75	0.04	0.08	69
SVM	No	0.60	1.00	0.75	102
	Yes	1.00	0.03	0.06	69
DT	No	0.97	0.97	0.97	116
	Yes	0.95	0.93	0.94	56

segment importance grid which may be wont to pick features. This framework is dreary to find the information is low and continuously exact.

6 Comparative Analysis

Treatment intensity and clinical features are condensed into a single measure to evaluate treatment effects in all forms of cancer on the downstream health consequences. The evaluation of their authors was first created for medical charts by clinicians. However, big studies for all research participants typically cannot access medical charts. A technique for assessing therapy intensity utilizing cancer registry [23]. This study aimed primarily to assess the link between the incidence of cancer and PM 2:5 exposure by >8:5 million U.S. registry cases of cancer. Secondary goals include assessing the relationships susceptibility to model selection, spatial check, and delay, as well as calculating the connection of exposure–response for different kinds of cancer [24]. The authors of [25] paper, SEER relative survival rates of breast, prostate, and colorectal cancer are declined at the county level in socioeconomic, demographic, and health factors. These models are first verified when comparing observed rates with anticipated rates in non-estimated counties. Long-term cancer survival and regional variations in survival varied with the disease location were the best indicators of education. Better breast and prostate survival than colorectal cancer have been anticipated. Data from cancer registries were gathered to provide national and domestic survival rate estimates for patients for ecological models. These estimates are valuable for prioritizing regions, where earlier diagnosis or greater access to healthcare is promoted and may also help assess the quality of the survival data gathered by cancer registries individually. Finally, in the last paper, the author revealed 34 papers applying machine learning for SEER cancer prediction. They retrieved data on their experimental configurations and scanned them for reproductive attempts. This review demonstrated that prior studies with various configurations have been conducted but that they do not have any simple repeatable cohorts and outcomes. In addition, no research by other institutions based on the same input data avoids transparent benchmarking. SEER data reproducible analysis is achievable and completely replicable survival prediction studies using logistic regression for breast and lung cancer are presented [26].

7 Conclusions

Exhibited that decision tree is moreover effective for human fundamental data assessment, and we can do pre-finding with no phenomenal clinical data. Soothsayer cancer development detection is done viably with AI counts with extraordinary precision. This can be moreover improved by using hybrid strategies of various classifiers similarly as by combining the correct logic. In this way, the proposed approach will yield a suitable procedure for both assumption and distinguishing proof. Accordingly, the work can fulfill the requirements of things to come also. Later on, we can work with more effective calculations and diverse patient information from assortments of nations.

References

1. Abid DM, Haque A, Hossain MK (2020) Factors causing stunting among under-five children in Bangladesh. In: International congress on information and communication technology. Springer, Singapore, pp 45–53
2. Vejendla LN, Gopi AP (2019) Avoiding interoperability and delay in healthcare monitoring system using blockchain technology. Rev d'Intell Artif 33(1):45–48
3. Chaitanya K, Venkateswarlu S (2016) Detection of blackhole & greyhole attacks in MANETs based on acknowledgement based approach. J Theor Appl Inf Technol 89(1):228
4. Patibandla RSML, Veeranjaneyulu N (2018) Performance analysis of partition and evolutionary clustering methods on various cluster validation criteria. Arab J Sci Eng 43:4379–4390
5. Lakshmi Patibandla RSM, Kurra SS, Veeranjaneyulu N (2015) A study on real-time business intelligence and big data. Inf Eng 4:1–6
6. Santhisri K, Lakshmi PRSM (2015) Comparative study on various security algorithms in cloud computing. Recent Trends Program Lang 2(1):1–6
7. Lakshmi PRSM, Sri KS, Bhujanga Rao MV (2017) Workload management through load balancing algorithm in scalable cloud. IJASTEMS 3(1):239–242
8. Patibandla RSML, Veeranjaneyulu N (2018) Explanatory & complex analysis of structured data to enrich data in analytical appliance. Int J Mod Trends Sci Technol 04(Special Issue 01):147–151
9. Dumala A, PallamSetty S (2019) Performance analysis of LAMAR routing protocol in VANET and MANET. Int J Comput Sci Eng (IJCSE) 7(5):1237–1242
10. Dumala A, PallamSetty S (2018) A comparative study of various mobility speeds of nodes on the performance of LAMAR in mobile adhoc network. Int J Comput Sci Eng (IJCSE) 6(9):192–198
11. Dumala A, PallamSetty S (2018) Investigating the Impact of IEEE 802.11 power saving mode on the performance of LAMAR routing protocol in MANETs. Int J Sci Res Comput Sci Manag Stud (IJARCSMS) 7(4)
12. Dumala A, PallamSetty S (2016) Analyzing the steady-state behavior of RIP and OSPF routing protocols in the context of link failure and link recovery in Wide Area Network. Int J Compu Sci Organ Trends (IJCOT) 34(2):19–22
13. Dumala A, PallamSetty S (2016) Investigating the impact of simulation time on convergence activity & duration of EIGRP, OSPF routing protocols under link failure and link recovery in WAN using OPNET modeller. Int J Comput Sci Trends Technol (IJCST) 4(5):38–42
14. Pavani V, Ramesh Babu I (2019) A novel method to optimize the computation overhead in cloud computing by using linear programming. Int J Res Anal Rev 6(2):820–830
15. Papasani A, Devarakonda N (2016) Improvement of AOMDV routing protocol in MANET and performance analysis of security attacks. Int J Res Comput Sci Eng 6(5):4674–4685
16. Reshmi Khader Bhai Sk, Suresh Babu K (2015) Big data search space reduction based on user perspective using map reduce. Int J Adv Technol Innov Res 07(18):3642–3647
17. Suresh Kumar BV, Reshmi Khader Bhai Sk (2018) BIG-IOT framework applications and challenges: a survey, vol 7, Issue VII, JULY/2018, pp 1257–1264
18. Sandhya Krishna P, Reshmi Khader Bhai Sk, Pavani V (2019) Unsupervised or supervised feature finding for study of products sentiment. Int J Adv Sci Technol 28(16)
19. Santhi Sri K, Prasad A (2013) A review of cloud computing and security issues at different levels in cloud computing. Int J Adv Comput Theory Eng 2:67–73

20. Santhi Sri K, Veeranjaneyulu N (2018) A novel key management using elliptic and Diffie-Hellman for managing users in cloud environment. Adv Model Anal B 61(2):106–112
21. Snow A et al (2021) Incidence of radiation-induced sarcoma attributable to radiotherapy in adults: a retrospective cohort study in the SEER cancer registries across 17 primary tumor sites. Cancer Epidemiol 70:101857
22. Comprehensive Cancer Information—National Cancer Institute, accessed 1 May 2021, from cancer.gov
23. Tobin JL et al (2020) Estimating cancer treatment intensity from SEER cancer registry data: methods and implications for population-based registry studies of pediatric cancers. Cancer Causes & Control 31(10):881–890
24. Coleman NC et al (2020) Fine particulate matter exposure and cancer incidence: analysis of SEER cancer registry data from 1992–2016. Environ Health Perspect 128(10):107004
25. Mariotto A et al (2020) Projecting SEER cancer survival rates to the US: an ecological regression approach. Cancer Causes & Control 13(2):101–111
26. Hegselmann S et al (2018) Reproducible survival prediction with SEER cancer data. In: Machine learning for healthcare conference. PMLR

Digitization and Society: Forms of Interaction and Expression

Valentina Milenkova, Boris Manov, and Dobrinka Peicheva

Abstract This article aims to reveal the digitalization as an integral part of the society. Every process, phenomenon, community and relationship is related to digitalization and information technology. This analysis presents different forms of symbiosis between society and digitalization. The objectives of the paper are to show specific dimensions of the advent of digitization and the various technologies in the Bulgarian society. The main research questions are related to the performance of high-tech level of Bulgarian online environment and focus on the main features of online learning, which are identified as new educational activities. Methodology of this article is based on results obtained from an online survey conducted in March 2021 with people of different ages, occupations and education. The survey questionnaire included topics that directly relate to the digitalization of society, the use of various digital devices and the Internet, participation in online education and attitudes toward it. The results obtained are indicators that digitalization of society is a real fact as well as that online learning has a place in the Bulgarian educational system. This article focuses on peoples' reactions, their assessments and views on ongoing online learning and its formatting. The whole article and the survey carried out are under the national project "*Digital Media Literacy in the context of "Knowledge Society": state and challenges*", № КП–06–Н25/4, funded by National Science Fund—Bulgaria.

Keywords Digitalization · Digital devises and skills · Online education · Digital literacy · Distance education

V. Milenkova (✉) · B. Manov · D. Peicheva
South-West University, 66 Iv. Mihailov Str., Blagoevgrad, Bulgaria
e-mail: vmilenkova@swu.bg

B. Manov
e-mail: bmanov@swu.bg

D. Peicheva
e-mail: peichevad@swu.bg

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_8

1 Introduction

Digitalization is an integral part of society. Every process, phenomenon, community and relationship is related to digitalization and information technology. The life of a modern person is a long series of active penetration of digital devices in our way of life, in our professional responsibilities and activities, in our free time and personal contacts. This strong digital saturation today is constantly recognized and modern person is clearly aware of his dependence on information technology, without which it would be difficult to do the job, to contact people and institutions that reflect different levels of social interaction, and to organize free time and entertainment. From this point of view, it is necessary to show the different forms of symbiosis between society and digitalization, as well as to emphasize the possible manifestations of this symbiosis.

The objectives of this paper are to show specific dimensions of the advent of digitization and the various technologies in the Bulgarian society and in particular:

- What digital devices do individuals have and how do they use them?
- How they get involved in the Internet and what is their participation in the various social networks?
- What is the quality of online learning as one of the examples of digital activity in social terms?
- What is the technological level of the online environment?

The main research questions are related to the performance of high-tech level of Bulgarian online environment and focus on the main features of online learning, which is a new educational activity for Bulgarian schools and universities and its basic actors gradually become active users of its.

The basic implication of the article is that in the Bulgarian context serious steps have been taken regarding the restructuring of modern university education in digital. At the same time, it should be emphasized that the digital education is a continuous process that follows the development of technology and in this sense there is a constant renewal and continuation.

2 Materials and Methods

The empirical basis of this article is based on results obtained from an online survey conducted in March 2021 with people of different ages, occupations and education. The survey questionnaire included topics that directly relate to the digitalization of society, the use of various digital devices and the Internet, participation in online education and attitudes toward it.

The survey included 1018 people, divided into the various categories:

Age

- 18–29 years: 37.9%
- 30–39 years: 24.6%
- 40–49 years: 18.7%
- 50–59 years: 8.4%
- 60+ years: 10.4%.

It is noteworthy that the most active age group in the sample are people under 40, who are digitally the most predisposed to the acquisition of digital skills and digital culture people. This is the generation of individuals who, as students or as parents of young children, are actively involved in various forms of interaction with information technology. They directly show and present their specific connection with the computer world of the "digital natives" generation [1].

Educational level was the other important feature of the sample including:

- Persons with education "up to secondary" which are: 1.4%
- Secondary school graduates make up: 35.6%
- Higher education graduates are: 41.1%
- The persons with scientific degree are: 22.0%.

It is noted that most are highly educated respondents. This is because digital skills also require a specific general culture and educational skills. Although there are many examples of people who have digital skills without being accompanied by higher education. In general, digital differences reproduce the divisions existing in society by age, ethnicity, profession, reinforcing and deepening them [2].

The sample included: Men: 28.7% and Women: 71.3%

In general, this distribution shows the priority of women as the most socially active part of Bulgarian society.

3 Results

The results presented in the paper are indicative of both the objective characteristics of different quantitative and qualitative conditions, opinions, assessments and views, which the respondents share. One of the important things in terms of digitization is the availability of digital devices that have become the main intermediary for the activity in the Internet, social networks and media. In the survey, most of the respondents possess:

- Mobile phone: 95.1% of the persons;
- Laptop: 90.2%
- Tablet: 42.9%
- Desktop computer: 39.2%
- Other: 13.9%

It addition, many respondents have more than one digital device, which is an indicator of the high degree of digitalization of the population. However, the question can be immediately raised here that although digital devices have already become cheaper, they represent a financial challenge for a large part of the Bulgarian population, given the high unemployment rate and the large share of people with incomes of the order of average salary for the country. In addition, it should be emphasized that in order for digital devices to be truly active, it is necessary to maintain an Internet service (connection), either as a plan included with the respective digital device, or as a stand-alone service purchased by the mobile operator. In this context, it can be said that digitalization reproduces existing divisions and inequalities by taking them to the next level. Maintaining the Internet connection proves to be of great importance for the use of the achievements of digitalization. In addition, depending on the positioning of the Internet connection used, summaries can be made about the extent of its use, as well as the activity of the network users themselves.

To the question "Where do you mainly use the Internet?" the answers received are as follows*:*

- At work: 4.1%
- At home: 16.1%
- Everywhere (I have mobile internet): 79.8%.

It is noticed that over 2/3 of the respondents have mobile Internet, which allows them to use it everywhere and to be as digital as possible, as they have access to the network at any time and in any place. In practice, these distributions are indicative of the fact that a large part of the Bulgarian population, mainly young people are connected at any time with their peers and colleagues at university or at work. What raises questions is that respondents who use the Internet at work have a relatively small share—only 4%. This means that most likely the nature of the activities performed does not require a network connection, or that there is no Internet in the respective workplace. This brings us once again to the topic of the divisions that digitalization reproduces and creates, and that divisions deepen personal backwardness or become a source of progress. Therefore, when talking about digitalization, we also take into account the extent to which people can use the Internet and its possibilities.

Another important topic related to digitalization is the expansion of the level of digital literacy. This is achieved both through personal training and through various courses that are attended. The level at which online learning takes place in an educational context is also important. The last two years—2020 and 2021 with small breaks were a time when classes in secondary and higher schools in our country took place in a digital environment. In fact, this is the topic that was the basis of the online discussions with students: about the quality of distance learning and its effectiveness. This topic is also present in the online survey because the majority of the Bulgarian population has a direct or indirect connection with online learning: as a student, as a parent, as a teacher in secondary or higher education or as a relative of any of these categories. In this sense, people with a stronger or weaker connection to online learning are in fact quite a high proportion. Therefore, we have included a series of questions related to online learning and its quality for several reasons.

- To understand what is the opinion about online learning of the majority of the Bulgarian population;
- To discuss the quality of online learning and the level of participation of young people in it.

Respondents were asked if the ongoing online training was of high quality. In addition to the positive and negative answers, the scale included the neutral answer "I have no opinion" in order to distinguish those respondents who, despite the wide range of related to online learning, are irrelevant and distanced from it for various reasons. According to the persons who answered, the distributions are as follows:

- 37.9% gave a positive answer, that online training was of high quality;
- 43.2% said "No"; 18, 9 have "no opinion".

These results show at least three trends:

- People who think that online learning is not of high quality are a little more than the respondents who gave a positive answer. And this is a problem for the level of education, learning and for the effectiveness of teaching and online activities.
- The difference between the positive and negative answer regarding the quality of online learning is not very big— it is 5.3%.
- Definitely need to make more effort to improve online learning and its possibilities.

In fact, the quality of education is a complex variable that has different components and depends on different things: teacher training, students' interest, technical security of the environment. So, it is necessary to have a broader understanding, because both the subjective and objective aspects must be emphasized. That is why we sought the assessment of the statement: "teachers cope with the requirements of online learning:

- Positively answered: 67.6% of the respondents;
- 15.9% of the persons gave a negative answer;
- 16.5% had no opinion.

These answers show that teachers are definitely assessed by the respondents as having the necessary digital skills and training to be able to conduct online training. This is particularly important because teachers are crucial figures in the overall distance learning and they depend both on what and how to teach, as well as how they assess their students. In fact, positive responses include the element of teaching and assessment, recreating the overall picture of the learning digital process [3].

The students themselves are the other important component of online learning-whether they manage to meet the requirements, whether they regularly prepare for online classes, whether they cope with the tasks [4]. The distributions in the answers to the question: "Do the learners cope with the online content?", are:

- 56.8% of the respondents answered positively;
- 26.5% answered in the negative;

- 16.7% of the surveyed persons do not have an opinion.
- In addition to this package of questions, another emphasis was added: learners have no difficulty with the online environment:
- 49.9% of the respondents answered positively;
- 30.3% of the persons give a negative answer;
- 19.8% have no opinion.

This emphasis was important to highlight the state of learners' digital skills and how these digital skills are applied in the learning process itself. It turns out that pupils and students are actually coping with the challenges of distance learning. As already mentioned, online learning and its implementation depend to a very large extent on the technological state of the environment: whether teachers and students have the necessary digital devices; what is the state of the Internet connection for both types of participants in distance learning; whether the digital platform used has the potential to take the necessary load when a hundred or more students enter the system, as is the case with high flows at some of the universities or schools; whether in cases where there are any problems with the platform or with its maintenance, these problems are fixed quickly? All the various aspects mentioned relate to the quality of the technological environment and 52.3% of respondents agree with this statement. It is definitely noticeable that the technological environment is evaluated positively. More than half of the respondents giving a positive answer, are indicators of a good assessment, as well as of the presence of good conditions for digitalization.

And in this context, the next logical point was: „Is online learning effective?"

- 39.9% answered positively;
- 41.7% gave a negative answer; 18.5% had no opinion.

It is noted that the difference between positive and negative answers is 1.8%, which means that the total number of people who evaluate the effectiveness of online learning in the two opposite poles is balanced. However, it should be emphasized that about 40% of respondents who agree that digital learning is effective are less than half, and this is not a very good sign. It should also be added that since the sample includes people from all over the country, there are regions where distance learning is really not very effective and there is no real learning process. Furthermore, for a this new form of learning, such as online learning, 40% approval is a relatively good result, especially considering that most parents do share their dissatisfaction with the distance education, saying that through online learning, in reality, their children do not study or study insufficiently.

In order to trace what in particular in digital learning is unacceptable and creates problems for learners, the questionnaire listed various shortcomings of online learning that respondents had to assess; respectively, we present the obtained results.

- No live contact in training: 87%
- Lack of communication between students: 74.6%
- Insufficiently good technological environment: 29.1%
- Insufficiently trained teachers—26.1%
- Learners face difficulties—38.8%

- The textbooks are adapted for face-to-face training—33.6%
- Online learning is expensive—3.7%.

In these responses, we note that the main disadvantage of online learning is the lack of communication with teachers: "live contact in learning" and "communication between learners themselves". It turns out that the social contacts that are established during the training both with the teachers and between the students are of great importance and in the results of the online survey they mark quite high values. In one case, the percentages reach close to 90%, and in the other case close to 80%. This shows the need for communication of networking, of living bond that creates the attendance training.

Next, when assessing the shortcomings of digital learning, "the difficulties that learners faced" come to the fore. Although the share of persons is less than half of the sample—38.8%, this answer is indicative that often during the training ambiguities arise, which for some of the learners need to be removed and the problems to be clarified. It turns out that the online environment is not conducive enough to seek additional explanations, or the other assumption is that most likely students can not focus on and understand the learning content. Obviously, some young people also have this problem—the inability to concentrate in front of the computer.

For some of the learners, various distractions arise, they do not understand the lesson at the moment, they do not want additional explanations because they think it is inconvenient to ask in front of everyone and so the gaps accumulate and these gaps later become ignorant. In many of the disciplines, knowledge is a continuum and there is continuity and connection; i.e., when there are misunderstandings or ambiguities and they are not filled, new ambiguities arise, which creates a long chain of learning problems. In the in person training, perhaps the environment itself creates more conditions and opportunities to ask after class or to seek contact with the teacher; although in person training students with poor grades, not understanding the study material or not making the necessary learning efforts were noticed.

In this regard, another component of in person training should be noted—"textbooks are adapted for face-to-face training" (33.6%), manuals also involve working in class. In general, the history of education has been related to the face-to-face forms and this tradition cannot be changed in a short time. Students, parents and teachers have such an attitude. Respectively, the percentage of people who indicated this answer is 1/3 of all persons.

"Insufficiently good technological environment" is cited as a difficulty in online learning of almost 1/3 of the sample—29.1%. This answer is indicative that not everywhere—at home, children have identical technological possibilities to be on the Internet and maintain a good connection. The issue of the divisions caused by digitalization has already been raised; and it will continue to attract attention.

"Insufficiently trained teachers" as a disadvantage of online learning is indicated by 26.1% of respondents. Undoubtedly, the lack of preparation of teachers to work in a digital environment becomes an unfavorable factor in conducting online classes.

One of the things that is not so important for the respondents is the “cost of digital learning“. This answer “Online learning is expensive” is given by only 3.7% of people in the survey.

Each of these factors undoubtedly affects the reduction of the attractiveness of online learning. These factors are of different essence—some of them are related to the nature of training, others related to its participants, others affect the technological characteristics of the environment. Taken together, these factors are indeed multifaceted, but they are important because they show in what aspect the active work of various educational institutions, the non-governmental sector, as well as at the management level—regional and national—should be deepened. It is obvious that online learning has established itself as a learning reality and will continue to have its significance, so it is important to improve it with a view to improving it in the future.

Therefore, as a deepening of the topic of the effectiveness of distance learning, the issue of the nature of the digital forms used was included. There is an understanding that just as in the classroom in face-to-face learning, there is a need to diversify the forms of teaching, so in online learning you need to think about innovative approaches, attracting attention, creating interactivity. Respondents were offered several different forms through which such diversity can be achieved and whether they are present in their online learning.

– Short-term videos for better perception (Tiktok, Instagram). They were mentioned by 14.5% of the persons, as finding a place in the online education process;
– Standard videos with explanatory content (YouTube, Facebook). This form was indicated as used in the training by 46.4% of the persons;
– Video lessons—indicated by 68.6% of the respondents;
– Other forms—39.7%.

The presented set of different forms shows that in the current online learning teachers from secondary and higher schools in our country are trying to create a diverse environment, to look for different opportunities to attract attention, to make learning more interactive and more understanding as content. In this context, two important circumstances can be highlighted. The fact that the majority of Bulgarian teachers in secondary and higher education in a short period of time had to acquire digital skills and be adequate to the online environment.

In March 2020 (the beginning of the COVID-19 pandemic), the percentage of those who could use digital platforms, create classrooms, create video tutorials, share the screen, etc., was small. Gradually, teachers became more confident as they expanded their digital skills by learning “step by step” and gradually their knowledge acquired relevant dimensions of the requirements of time and learners. The second important circumstance, which must also be taken into account, is related to the age of the teachers, both in the secondary and in the higher schools in Bulgarian conditions. The high percentage of adult educators means difficulties with the acquisition of digital skills, which are of great importance in the online process. In this sense, the rejuvenation of the teaching staff or the setting of requirements for digital literacy above the basic level, which should be linked to the remuneration of teachers, is a milestone in the work and a criterion for qualitative digital teaching skills and training.

4 Conclusion

Based on the results obtained from the survey, several conclusions can be drawn. Digitalization has a place in Bulgarian society and it is at a good level. The online learning is assessed relatively positively, it is perceived as a good step and solution and people evaluate it as a main element of the educational space. One of the advantages of online learning is its flexibility. Instead of training taking place in a fixed place and time, with the help of high technology it can take place anywhere and at any time. Online education uses a variety of forms of expression—video, audio, text, tests, etc., which in turn could lead to higher engagement and efficiency in understanding, remembering and reflecting information, as it helps participants with different learning styles. The consequences of the change in the way of learning in school and university education can be found both in the psychological and emotional state of the students and in the quality of the education they will receive [5].

A main conclusion of this article is that various improvements need to be made to make the online education activity more effective. The most important thing to think about is how to overcome the shortcomings of online learning and how to deal with them for people of different ages and statuses.

Acknowledgements The article has been developed in the framework of the research project "Digital Media Literacy in the context of "Knowledge Society": state and challenges" № КП–06–H25/4, funded by National Science Fund—Bulgaria.

References

1. Erstad O (2010) Educating the digital generation. Nordic J Digit Lit 1:56–70
2. van Deursen AJAM, van Dijk JAGM (2009) Using the internet: Skill related problems in users' online behavior. Interact Comput 21(5):393–402
3. Sefton-Green J, Nixon H, Erstad O (2009) Reviewing approaches and perspectives on "digital literacy". Pedagogies 4(2):107–125
4. Milenkova V, Keranova D, Peicheva D (2020) Digital skills, new media and information literacy as a conditions of digitization. In: Applied human factors and ergonomics (AHFEE 2019). Springer, pp 65–72
5. Eshet-Alkalai Y, Chajut E (2009) Changes over time in digital literacy. Cyberpsychol Behav 12(6):713–715

E-Managing the Pre-election Messages During the 2021 Parliamentary Campaigns in Bulgaria

Neli Velinova, Mariyan Tomov, Lilia Raycheva, and Lora Metanova

Abstract The pre-election campaign for the early parliamentary vote in Bulgaria on July 11, 2021 was held in the conditions of an uncertain COVID-19 situation, political confrontation and the games of the European Football Championship. Following the trend of the previous regular elections of April 4 after which no government was appointed, Internet platforms and especially social networks have become increasingly popular channels for politicians to communicate with voters. The aim of the study focuses on the dynamics of pre-election online communication. The object is the specifics of the Internet connection between the audiences and the candidates for members of Parliament during the election campaign in July compared to the previous one in April. The subject refers to the digital election messages of the leaders of the political forces, presented in their Facebook profiles. The methodology is an empirical study and comparative analysis. The scope includes those political forces that have passed the 4% electoral threshold. The results are indicative for those interested in digital political communication during social isolation of pandemic.

Keywords Digital communication · Social isolation · Pre-election messages · Social networks · Pre-election parliamentary campaign

1 Introduction

During the period of democratization—since 1989, the election campaigns in Bulgaria have developed in parallel with the demonopolization, liberalization and transformation of the media system. Nevertheless, the deregulation of the radio and television broadcasting sector was protracted, giving way to the rise of two interrelated processes—politicization of the media and mediatization of politics [1]. Since the beginning of the new century, these processes have accelerated with

N. Velinova (✉) · M. Tomov · L. Raycheva · L. Metanova
The St. Kliment Ohridski Sofia University, Sofia, Bulgaria
e-mail: nelikdkd@gmail.com

L. Metanova
e-mail: loranikolova@abv.bg

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_9

the widespread use of digital technologies in everyday communication. However, radio and television, despite their simultaneity, are drastically lagging behind in the high-speed race for consumers' attention.

The deficits of democratization feed the ground for the development of populism as a political concept and rhetorical style. Nowadays constant migration between political actors, which escalates in the use of populist approaches, characterizes the political environment in Bulgaria. In fact, the use of populist phraseology is evident in all political forces in the country, whether left or right. Political leaders and parties with pronounced populist behavior have mixed, often changing characteristics.

The messages of the political actors address the audiences mostly through the media. Populists' strong criticism of the status quo and the chimera of democracy usually intertwine with the function of the media as a corrective factor in relation to public authorities. The growing impact of social networks on the process of communication between the public and political formations generates a reasonable assumption that this model of interaction will develop, especially in the realities of social isolation, such as that caused by the COVID-19 pandemic. That is why it is especially important to outline the trends and peculiarities in the development of these relations in the context of the dynamics of the pre-election online communication between politicians and the public.

2 Methodology

The research, undertaken by an academic team from the Sofia University "St. Kliment Ohridski" in two stages (04.03.-04.04.2021, and 11.06.-11.07.2021), is focused on the dynamics of the pre-election online communication between politicians and the publics in both the 2021 elections for a national parliament. It draws on the framework and results of the analysis of the April regular vote compared to the July early elections in the context of the epidemic caused by COVID-19 [2].

The object is the specifics of the Internet connection between the modern digital audiences and the candidates for MPs during the two election campaigns (April and July 2021) in Bulgaria. The subject refers to the digital election messages of the leaders of the political forces, presented in their Facebook profiles during the one-month election campaign. The methodology is an empirical study and comparative analysis. The scope of observation includes political forces that have crossed the 4% electoral threshold.

The study examines the verbal and non-verbal communication of candidates, the quality of their messages in terms of positivity, negativity or neutrality, as well as their commitment to social, health, economic, technological and other important issues related to the welfare of the population in a country—member state of the European Union. The frequency of Facebook use by political leaders, the dominant issues in their messages, as well as the digital activity of the audiences have also been monitored.

3 Results

In the more than three decades since the democratization process began in 1989 eleven parliamentary elections (1990, 1991, 1994, 1997, 2001, 2005, 2009, 2013, 2017 and 2021—2: 1 regular and 1 early) were held and eleven governments appointed, of which only four have completed a full four-year term of office and seven were caretaker cabinets. This shows a worrying deficit of representative democracy in Bulgaria.

The early elections for the national parliament in July 2021, like the previous regular ones in April, were held in a situation of global insecurity in such social spheres as healthcare, economy, politics and others. The only legislative result of the 45th National Assembly, which lasted less than a month, was the hastily revised Electoral Code, voted on the eve of Good Friday, contrary to the Rules of Procedure, but with the intention of ensuring greater fairness of the vote. A new Central Election Commission was appointed, compulsory machine voting has been introduced for sections with more than 300 voters, and the restriction of 35 sections in non-EU countries has been lifted.

Although the early elections in July were the most expensive in the country's electoral history, turnout was unusually low—42.19% or 8.42% less than the regular vote in April [3]. The activity of early voting seemed to disprove the effectiveness of the massive introduction of machine voting. Thus, only 38% of those obliged to vote with machines in sections with 300 or more voters went to the polls, while significantly more—55%, were those who voted with paper ballots. Resistance to machines refused many to go to the polls. Preventive actions by law enforcement agencies in places where there were suspicions of controlled voting, although loudly announced, were not sufficiently fair and effective.

The wisdom of the Bulgarian people gave a second chance to those political forces elected in April, without again having the upper hand of any political formation.

If for the regular elections in April the participating political entities could be divided into two: parliamentary (Coalition *Citizens for European Development of Bulgaria–CEDB/Union of Democratic Forces–UDF;* Coalition *Bulgarian Socialist Party-BSP for Bulgaria,* and political party *Movement for Rights and Freedoms-MRF*) and non-parliamentary (political party *There Are Such People*, Coalition *Democratic Bulgaria-DB* and Coalition *Stand up! Goons out!-SUGO*), in the July déjà vu all six ranked equalized as parliamentary represented, regardless of the time of their stay in the National Assembly or the effectiveness of their activities in it for the formation of policies and legislation ensuring sustainable development of the country.

All participants in the election campaign, both in the regular and in the early vote, and not only those who crossed the 4% barrier, have bet extremely seriously on their presence on the social network Facebook during both one-month campaigns. The candidates who ran for the 240 seats in the National Assembly for the early vote in July did not differ significantly from the ones for the regular vote in April: 64 (vs. 71) were the political formations organized in 15 (vs. 18) political parties, 8 (vs. 12) coalitions and 1 independent candidate. In the remake, the winners were again the same—two parties and four coalitions, representing 33 political entities, formed the 46th Parliament. However, the change in the rules led to a shift in the ranking. And not only that: the massive negative rhetoric against the former ruling *CEDB-UDF* coalition by all ranked political formations, by the President and by some ministers of the caretaker government and during the campaign period contributed to this (Figs. 1 and 2).

There are such people became the leader, winning 14 new seats, 3 of which from the vote abroad. *Democratic Bulgaria* also increased its score by 7 seats, incl. one from abroad and ranked fourth, displacing the *MRF,* which remained fifth and won 1st place in the vote abroad, but reduced its result by 1 MP—from 30 to 29. The *CEDB-UDF* coalition lost the most—12 seats, although it ranked second. *BSP for Bulgaria* retained its third position, but lost 7 seats. *Stand up! Goons out!* Which was renamed to *Stand up! We are coming!* Was again last, with one MP less—from 14 to 13.

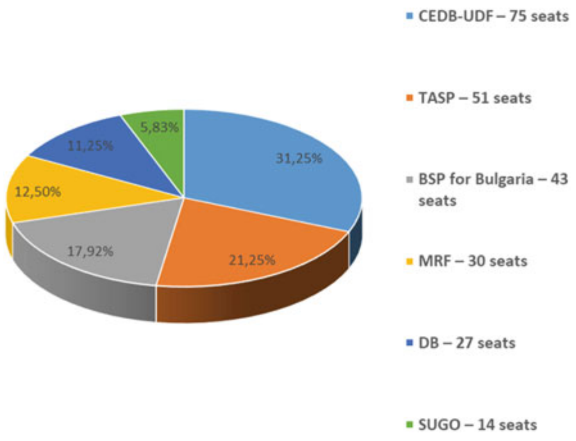


Fig. 1 Election results (04.04.2021)

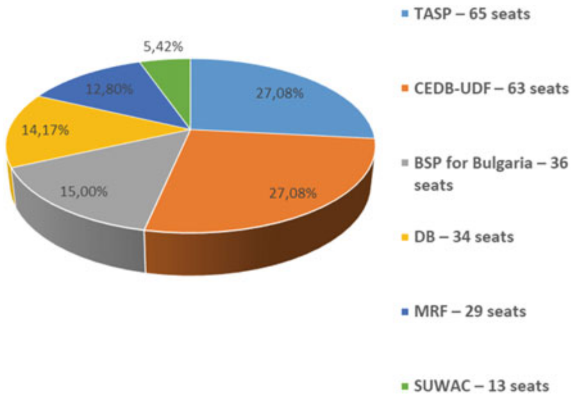


Fig. 2 Election results (11.07.2021)

During the early parliamentary elections, 3,973,856 registered voters (57.81%) were not represented in the 46th National Assembly, which is a challenge to its legitimacy. All these people were not asked about the program and composition of the government, nor how to outline the priorities for governing the country, which is counterproductive for democracy. Obviously, most Bulgarians refused to comply with media, political and sociological propaganda, especially when they did not meet their needs. It seems that their idea of a democracy in which causes, values and principles are upheld was undermined by the wave of populism, defending interests and unfulfillable promises, skillfully playing with people's fears and hopes. Fairly criticizing previous managerial shortcomings, the populists had no vision of proposing a meaningful program for their change and energy to implement it. And any social change is a long, consensual process, not a momentary "erasure" of the political legacy (both good and bad). The remake of the neglect of the dialog, of the belittled prioritization of the public order, leads to the replacement of the people's discontent by a fake democracy.

All participants in the election campaign, both in the regular and in the early vote, and not only those who crossed the 4% barrier, have bet extremely seriously on their presence on the social network Facebook, during both one-month campaigns.

Following the aim of this study, focused on the dynamics of pre-election online communication in the two parliamentary votes in 2021, the messages of the leaders of political parties presented in their Facebook profiles during the one-month campaign for the regular elections (04.04.2021) and for the early voting (11.06.-11.07.2021) were examined and compared. Due to the limited size of this article, the results will be presented only for those political forces that have crossed the 4% barrier.

The Facebook campaign of the leader of *There are such people* Slavi Trifonov is perhaps best characterized in Katherine Calvait's comment in Süddeutsche Zeitung: "A model for success? More mockery. Trifonov, musician, presenter, TV star, neo-politician, no program. During the election campaign, he hardly showed up, his ideas were deliberately formulated in a vague way. Now that he can form a coalition with other reformist forces and will have to present a government program, he comes up with conditions that cannot be met, so the question arises: Is the man a visionary or a charlatan?" [4].

Overall, the campaigns of Boyko Borisov—the leader of the coalition *CEDB-UDF* and former Prime Minister's Facebook page were rational and pragmatic. He was trying to play the role of a unifier of the nation. In both campaigns, among the posts published on his Facebook page were listed those of some European leaders who declared their support for him, such as the one by Manfred Weber, the chairman of the Group of the European People's Party in the European Parliament.

The Facebook profile of the leader of the Coalition *BSP for Bulgaria* Cornelia Ninova in both campaigns was moderate in intensity. The key words of her messages were predictability and stability.

The coalition *Democratic Bulgaria* has two chairpersons. The campaign of one of them—Hristo Ivanov on his official Facebook page for the elections on July 11 does not differ in style from that of the regular vote on April 4, 2021. He relies on expert speech, not so much on emotional personal posts. The main message is the need for change and the statement that the *DB* coalition knows how to make this change. In general, the style and approach of the online campaign on Facebook of the other co-chairman of the *DB* coalition Atanas Atanasov also did not differ much from the campaign for the parliamentary elections on April 4, 2021. He also relies on a rational rather than emotional approach. Most of his posts are related to links to interviews and media publications.

The Facebook profile of the leader of the political party *MRF* Mustafa Karadayi is characterized by an unobtrusive and casual election strategy. Verbal communication is almost non-existent in both election campaigns. The agitation is reduced to modest photos and videos. There is no tension from the upcoming race, but rather confidence. It seems that the *MRF* leader does not rely only on the election campaign on the social network, but rather on a hard electorate.

The Facebook page of the leader of the coalition *SUGO/SUWAC* Maya Manolova is very active but it is dominated by populist promises. The short, meaningless life of the 45th parliament in Bulgaria shows the political weakness of the MPs, who failed to realize the key role of the political institution in representative democracies.

The comparative study of the two election campaigns (for the regular vote in April and for the early one in July) analyzes the verbal and non-verbal communication of the leaders of the political forces, overcoming the 4% barrier. The quality of their messages on Facebook in terms of positivity, negativity or neutrality, as well as their commitment to social, health, economic, technological and other important issues related to the welfare of the population in the country as a Member State of the European Union were also studied. Moreover, the digital activity of the audience was also monitored.

The results of the analysis show that during the election campaign Bulgarians preferred to be informed first by television, and then—by social networks—mostly—by Facebook. Online communication replaced live political contacts with the public, and the numerous likes, comments and shares expanded the boundaries of the audiences. However, the number of publications, the frequency of use of the social network, as well as the invested funds did not turn out to be directly proportional to the achieved success. Judging by the quality of the content of the posts, relying on populism in its various dimensions was the most profitable strategy. For some of the new political formations, aggressive rhetoric was also effective. In a few of the Facebook profiles surveyed, political leaders clearly set out their intentions so that voters had the opportunity to make informed choices.

The common conclusion for both campaigns is that the populist and emotional messages of the long time TV showman Slavi Trifonov—leader of the political party *There are such people*—were formed around the position of "anti status quo", the importance of people's opinions, patriotism and national pride. Although the publications are few, his page is popular—the interactions are several thousand.

In general, the rational, pragmatic campaign is leading on the Facebook page of the leader of the Coalition *CEDB-UDF* Boyko Borissov. The scale of the work conducted by the governments led by him was predominantly represented.

The Facebook profile of the leader of the *BSP for Bulgaria* Coalition Cornelia Ninova was moderate in intensity. The key words of the crisis management Coalition's messages were predictability and stability.

The election campaign of the political party *Movement for Rights and Freedoms* was extremely modest in the Facebook profile of its leader Mustafa Karadayi and passed under the motto "Restart of Statehood". As a strategy, the *MRF* did not rely heavily on the publicity created by the social network to increase the number of its voters.

The messages in the election campaign of the Coalition *Democratic Bulgaria* adhere to political topics through expert speech, and not through emotional speech or other techniques. The Facebook profiles of the two co-chairs Hristo Ivanov and Atanas Atanasov follow this line of communication with the voters.

And the coalition *Stand up! We are coming!* Relied on its leaders' Facebook activity—Maya Manolova in June-July, together with Nikolay Hadjigenov in March–April. The campaign had a very populist flavor. Despite the tireless work and energy to attract a stable electorate, the results of the Coalition did not show much success.

Coincidentally or not, the President scheduled both votes on days that do not stimulate the turnout—04.04.21 coincided with the Catholic Easter, and 11.07.21—with the finals of the European Football Championship. Although the number of polling stations in countries outside the European Union has increased for the early voting, the last-minute compulsory machine vote for sections with more than 300 voters had not a positive effect on voter turnout. The election in July was too expensive and unrepresentative—57.81% of the registered voters or 3,973,856 did not go to the polls. In other words, the leading *There are such people* represents 9.57% of all registered voters, the second-placed *CEDB-UDF* coalition—9.34%, the third-placed coalition *BSP for Bulgaria*—5.32%, the fourth-placed coalition *Democratic Bulgaria*—5.02%, the fifth-ranked political party *MRF*—4.26% and the last, sixth political force *Stand up! We are coming!*—1.99%. The total legitimacy of all elected political forces in the 46th National Assembly is 35.5%, or nearly twice as many are those registered voters—4,571,068 (64.5%) who have no political representation, compared to 2,302,716 who had, although highly fragmented, an extremely difficult obligation to create effective policies in the interest of the people.

4 Conclusion

The dynamics of the election campaign of the participants in the race for both the 45th and the 46th National Assembly show that neither the amount of funds invested in political advertising, nor the scope of media and online activity, nor populism in its various dimensions are sufficient for electoral success. Deficits in the quality of advertising forms, in the clarity of party programs, and in the purposefulness of the messages are the more serious challenge to the informed choice of voters.

The counterproductive behavior of the 45th National Assembly led to a remake of the campaign for early voting, which offered déjà vu messages, continued neglect of dialog, underestimated prioritization of public agenda, and the faking of democracy. The 46th National Assembly also failed to form a regular government, and new parliamentary elections were scheduled for November 14, along with a presidential one.

The results of the study are indicative of those who are interested in digital political pre-election communication in the context of the social isolation of the COVID-19 pandemic.

Acknowledgements The paper has been developed within the framework of the academic research projects КP-06-COST/5—18. 06. 2019 and KP-06-M35/4-18.12.2019 of the National Scientific Fund of Bulgaria.

References

1. Raycheva L (2014) Mediatization of politics VS politicization of media in the situation of an election campaign. In: Krumov K, Kamenova M, Radovich-Markovich M (eds) Personality and society: the challenges of change. Bulgarian Academy of Sciences and Arts, Serbian Royal Academy of Sciences and Arts, European Center of Business, Education and Science, Sofia, pp 75–98
2. Neli V, Mariyan T, Lilia R, Lora M (2021) Digitization of pre-election messages during the 2021 parliamentary campaign in Bulgaria. Paper presented at the International conference on human systems engineering and design: future trends and applications (IHSED 2021), September 23–25, Dubrovnik, Croatia
3. Central Election Commission of the Republic of Bulgaria (2021) Parliamentary elections. https://www.cik.bg
4. Kahlweit C (2021) Hauptsache, alles anders. https://www.sueddeutsche.de/meinung/bulgarien-slawi-trifonow-parlamentswahl-1.5351874

Highly Stochastic Time Series Modeling using HTM in Comparison with Commonly Used Methods

Filip Begiełło and Tomasz Bławucki

Abstract This study compares the HTM models applicability in highly stochastic time series forecasting problems, to a range of commonly used approaches. The models were tested on a real-world data, representing raw material usage in a food processing company. The comparison was done on a set of 21 data series with a high disparity of underlying process characteristics. HTM models were evaluated against 6 other approaches. As a result, HTM models were able to outperform other models in 8 out of 21 cases, with an average improvement of around 20% of RMSE value, scoring in the first place as a most accurate approach.

Keywords Time series · Forecasting techniques · Stochastic data modeling · Hierarchical temporal memory · HTM · Machine learning · Deep learning · Data science

1 Introduction

Modeling and forecasting of time series are a highly explored and important task in modern research. Many crucial data take form of a time series and need to be predicted accurately. A proper analysis of a time series allows a higher level of understanding when it comes to the modeled process. To achieve this goal, a particular emphasis needs to be placed on choosing an adequate modeling method to properly describe the underlying structure and connections existing between the data points [1].

Two approaches can be distinguished when it comes to modeling time series: time domain approach—based on correlation and autocorrelation analysis, and frequency domain approach—reducing time series to a set of component features, each described by its frequency, amplitude, and phase offset. Both approaches allow for accurate time series analysis and moreover can be successfully combined to

F. Begiełło (✉) · T. Bławucki
Smart Geometries Sp. z o.o., Lęborska 8/10/183, Warszawa, Poland
e-mail: f.begiello@smartgeometries.pl

T. Bławucki
e-mail: t.blawucki@smartgeometries.pl

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_10

achieve better results [2, 3]. Another way to categorize models is their ability to represent nonlinear dependencies in the data, hence linear and nonlinear models [4].

When it comes to forecasting, linear models were widely used up until recently, due to their relative accuracy and transparency, or in other words, ease of explanation, when it comes to the cause of prediction [2, 4]. With the advent of easily available large datasets and higher computing power, it became possible to better utilize the potential of nonlinear models such as deep neural nets [5]. Those techniques have been used widely, not only for time series forecasting, but other highly complicated tasks such as face recognition, cancer diagnosis, or crops harvest automation [6–8].

The problem of constructing an accurate model becomes even more pronounced when it comes to time series with high level of noise or one representing a highly stochastic process. In such cases, both linear and nonlinear models can struggle to generate accurate predictions, albeit due to different problems [1, 4].

Hierarchical temporal memory, or HTM for short, is a novel machine learning technology developed by Numenta. It is designed to closely emulate the structure and processing capabilities of a neocortex, focusing especially on its pattern recognition and sequence learning abilities [9]. Due to its architecture, a HTM model should be highly stable and resistant to noise, without sacrificing any predictive capabilities [9–11]. Those characteristics make HTM models a perfect candidate for highly stochastic time series forecasting.

The aim of the paper is to examine how the HTM models compare to other, already established forecasting methods when applied to predicting a real, highly stochastic time series.

The rest of the paper is structured as follows. Section 2 presents methods and models used during the course of the study. Section 3 describes the experiment framework—dataset used and data processing as well as training procedures. Section 4 presents the results. Discussion and conclusion are covered in the Sect. 5.

2 Time Series Forecasting Methods

2.1 Commonly Used Approaches

During the course of the study, a representative group of commonly used models, both linear and nonlinear, was used. Among the linear methods were ARIMA, Holt-Winters seasonal method, and machine learning models. From nonlinear, two approaches were chosen—deep neural networks and transformer model. Lastly, an approach based on analysis of component signals, extracted with Fourier transform, was added to the comparison.

Autoregressive Moving Average Models Autoregressive moving average models (ARIMA) and its more complex variant—seasonal autoregressive moving average (SARIMA) are one of the most known and widely used methods in time series and forecasting tasks [12]. Both ARIMA and SARIMA models are providing good prediction accuracy and flexibility when it comes to representing various types of time series, although it is necessary to check a series of statistical tests and apply transformations to achieve a stationary form of the analyzed dataset beforehand. ARIMA models find a wide range of applications, such as power engineering [13], flooding prevention [14, 15], forecasting macroeconomic indicators [16], or predicting future sales level [17].

Exponential Smoothing Models When modeling a time series with a strong cyclic trend, a commonly used method is exponential smoothing algorithm. It is a simple and stable method for time series forecasting, often performing better than more complex models [18]. The idea behind this approach is to continuously revise a forecast using the most recent data points as the model progresses. Exponential smoothing method assigns exponentially decreasing weights to older observations, while recent observations are given relatively higher weights [19]. Models based on this approach are used throughout multiple industry sectors like power engineering, fossil fuels, or tourism, where proper and accurate forecasts are crucial in tasks such as production optimization, store management, or advertising campaign planning [20–23].

Holt-Winters method (H-W) is one of such models. This method is used when the data clearly show signs of trend and seasonality. Depending on the type of modeled seasonality type, this approach can be further divided into multiplicative seasonal models and additive seasonal models [19, 21].

Fast Fourier Transform Model The discrete Fourier transform (DFT) is an efficient algorithm for computing the Fourier transform of a discrete data series. The usual application of it is to analyze main frequency components, filter noise, or compress signals to achieve theirs minimal representation [24, 25].

A novel approach is to use DFT as a tool for time series regression. Given a series, decomposed to frequencies and magnitudes, its most important components can be chosen and the inverse DFT calculated to re-generate a time series of desired length. This approach is effective for medium length and short length series [26, 27]. DFT regression accuracy on series with strong cyclic and seasonal changes is often competitive to more complex methods like autoregressive moving average, or machine learning models [28, 29]. This technique finds use in critical resources management [29, 30] and in stock index prediction tasks [25].

Machine Learning Models Employing machine learning (ML) models for tasks like time series clustering, classification, or forecasting are becoming more and more popular. Very often this data driven approach, in which models are given enough of lightly preprocessed data, offers superior accuracy compared to classical statistical approaches [31–33].

When it comes to forecasting a time series with ML models, this task falls under classification as a supervised learning problem, in which the model is trained on a finite set of subsamples, taken from the original series. This process relies on an initial assumption that there are some dependencies between modeled process and chosen input variables, so the proper selection of those is critical. During the model fitting phase, the impact of those input variables on the modeled process is established and saved as a set of weights representing those relationships. Once the mapping is set, the model can be used in the forecasting process [32, 34].

Deep Learning Artificial neural networks (ANNs) are a recently dynamically developing extension of machine learning models. This kind of models require a significant amount of hardware resources and data, but in exchange, offer a natural ability to represent nonlinear dependencies in data, and as such have a great potential to solve complicated problems, beyond the capabilities of previously presented methods [35]. Their multipurpose character allows ANNs to be used in both univariate and multivariate, as well as single and multi-step prediction problems [36]. Additionally, tasks already solved by autoregressive moving average models can also be relegated to neural networks [37]. ANN models are also widely used in image recognition tasks, natural language processing, stock market prediction, power grid electricity load forecasting, fraud detection, air pollution prediction, robotics, and many others [38–41].

A variety of unique ANN architectures were developed, but when it comes to modeling a time series, two distinct variants appear to be the most popular:

Long-Short Time Memory (LSTM) A variant of recurrent neural network, which resolves the problem of vanishing and exploding gradients, extending the memorizing capabilities of the network when compared to classic recurrent ANNs. Management of long-term temporal dependencies in data gives LSTM great capabilities of modeling complex time series, especially when combined with additional, exogenous data [42].

Transformer (TF) Unlike sequence-aligned models, this model does not process data in an ordered series manner, instead the sequence is processed as one chunk of data. Order information is encoded inside the model, using self-attention mechanisms [43]. Due to this, transformer-based models have the potential to capture the complex dynamics of time series data, which are challenging for sequence models. This architecture, with some minor changes, can be efficiently used in very long sequence time series forecasting tasks [44, 45].

2.2 *Hierarchical Temporal Memory*

The hierarchical temporal memory (HTM) model finds its root in a theoretical framework called the Thousand Brains Theory of Intelligence, and more precisely, the properties of the neocortex proposed in it. It is based on an assumption, that by emulating some of the features of the neocortex structure, especially the way neocortical neurons are organized, a general-purpose AI model can be developed [46].

HTM model relays on a series of neurons organized into columns. All of the columns and neurons are structurally the same, but differ when it comes to connections between them, which are developed during the training process and form the memory mechanism that allows them to recognize multiple complicated patterns [46, 47]. This mimics the structure of neocortex, which is mostly structurally uniform as well, despite its regions being able to perform a plethora of specialized tasks [46].

The described mechanism is possible due to the departure from the simple artificial neuron that is a basis of multiple currently employed neural network models. A HTM neuron is closely resembling a pyramidal neuron—the type of excitatory neurons present in the neocortex. As such, it can be divided into two zones, proximal zone, that represents the feed-forward input, and distal zone, containing multiple connections to both neurons in the same regions providing the context, and feedback connections from other regions [9, 48]. In this way, a neuron reacts to a current input and can stimulate other neurons, it is connected to. Depending on which connections are active, a neuron can be in an active state—the cell is activated by a current input, a predictive state—the cell might become active due to the next input, or inactive state. The neurons output can only be binary [49] (Fig. 1).

Following the HTM structure, all the neurons are organized into columns. Each column consists of the same number of neurons and receives the same feed-forward input [47]. A column has the potential to be in active state, if any number of the neurons it comprises of becomes active, otherwise it stays inactive. Each combination of active columns corresponds to a single value, or rather, a pattern of input bits it encodes. Those combinations emerge during the first step of the training process [48] (Fig. 2).

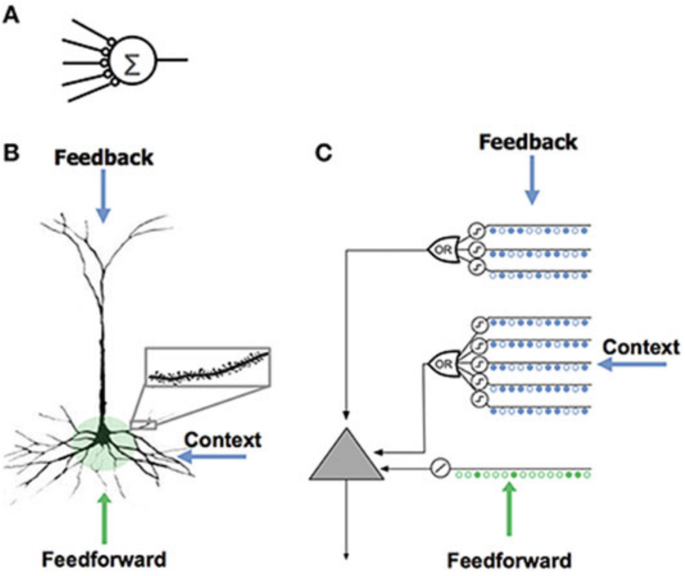


Fig.1 Comparison of a classical artificial neuron (**a**) pyramidal neuron (**b**) and HTM neuron (**c**). *Source* [49]

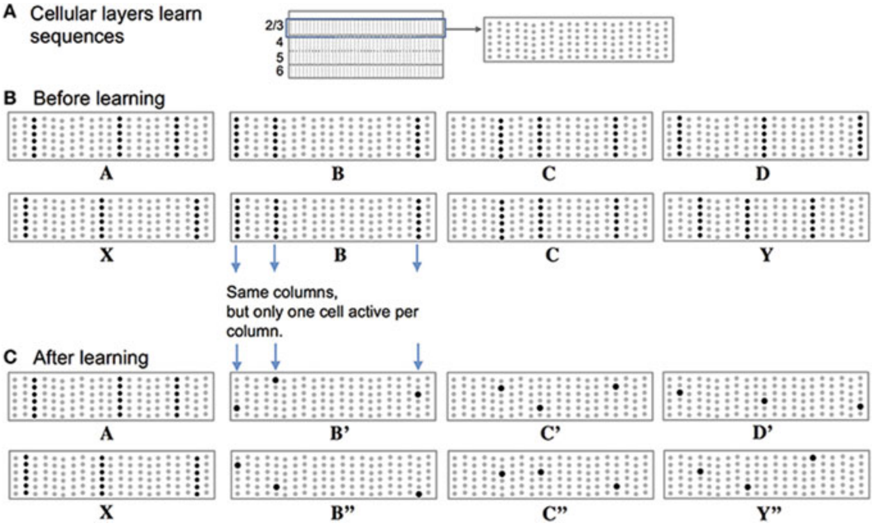

A Cellular layers learn sequences
2/3
4
5
6
B Before learning
A
B
C
D
X
B
C
Y
Same columns, but only one cell active per column.
C After learning
A
B'
C'
D'
X
B"
C"
Y"

Fig. 2 Visualization of the training process for the HTM model. *Source* [49]

The next step consists of gradually building and strengthening the connections between neurons in columns activating in sequence, as to allow the neuron in predictive state to properly forecast what value comes next. This includes reducing the number of neurons activating in each column from all to a necessary minimum [48, 49]. Due to this, each encoded by active columns value can be properly understood and predicted in different series, since a single column may be activated by one of many belonging to it neurons signifying a different context.

An important part of the HTM model is its inner representation of data, which ties to its ability to reduce a number of active neurons in columns. Since in a neocortex the analyzed patterns appear to be represented only by a small portion of neurons active at the same time, HTMs follow a similar approach [50]. This data format is called a sparse distributed representation (SDR). It assumes that at high-enough dimensionality, only a fraction of space (usually around 2% according to literature [9, 49, 50]) needs to be used at once to encode an information. Using SDR proves to not only improve robustness and stability, when it comes to a highly noisy data encoding, but also positively affects learning speed and computational efficiency [10, 50].

To further improve the benefits of SDRs in HTM models, an initial module called the spatial pooler is used. Its role is to convert an arbitrarily encoded binary input into an SDR through a combination of competitive Hebbian learning rules and homeostatic excitability control [11].

3 Experiment Framework

3.1 Problem Formulation

When it comes to real-world data, most of the analyzed time series are highly stochastic due to plethora of external variables influencing the modeled process. In this study, we try to apply a recent and less explored approach—namely HTM models, to predicting such data in comparison with other, widely used and proven methods.

3.2 Dataset Description

Since we attempt to research a possibility of predicting a highly stochastic process at a commercially acceptable prediction accuracy level, as our dataset, we have chosen 21 raw material indices (SKU). This data were provided by a non-disclosed international food processing and manufacturing company and represent a real usage in a production process. Each index is unique regarding the past usage characteristics. Individual SKU usage history varies in: usage history length, usage stability over time, outlier observation presence, and outliers occurrence frequency and stationarity. Additionally, throughout the SKUs, we can observe a number of different trends—some of them are characterized by a constant usage growth over time, others maintain a stable level of it, or in some cases, the demand is slowly decaying (Fig. 3).

Time series data are aggregated as weekly usage values—quantity of material used in a particular week is the sum of all observations within this period, assuming Sunday as the first day of the week. In addition, the data have been extended with date time information, connected to each of the weekly usage values.

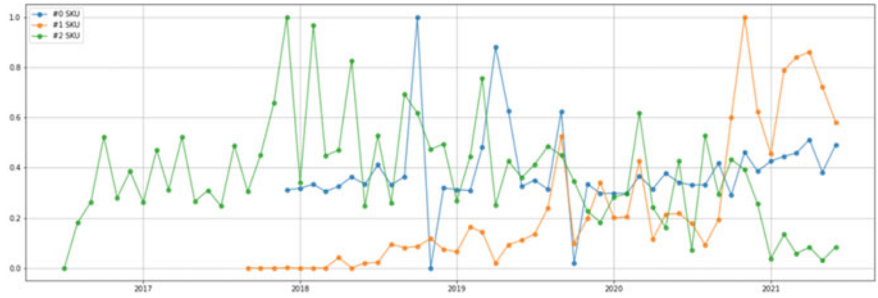


Fig. 3 Representative group of 3 out of 21 SKUs. The usage values have been rescaled for the purpose of visualization

3.3 Preprocessing and Training Process

The preprocessing and training process differed slightly, depending on the model, since a wide range of types of approaches were used in the comparison.

Due to the nature of the data, it was necessary to fill values with zeroes, for the days missing due to no material usage. In addition, the data were resampled, to achieve the predetermined granulation of one week. This was done for each of the approaches.

To help the process of fitting, for machine learning, SARIMA, and Holt-Winters models, each of the data series was scaled individually using MIN–MAX scaler. It is important to note that maximal and minimal values were established on the training set, but the transformation was performed on the whole time series—both the training and validation sets. To remove the solitary, outlying data points that could disrupt the training process, an anomaly filtering and log transformation were performed on the data. This procedure was beneficial for all of the classical approaches, which are all to a degree sensitive to being skewed by outliers and require the data distribution to be as close as possible to Gaussian distribution. For the models that require data series to be stationary, or as close to it as possible (SARIMA, Holt-Winters, linear ML models), the data were transformed to the form of the first difference of the original series. Seasonal component of the date was encoded with radial basis function (RBF). In the case of linear machine learning models that due to their limitations are unable to perform time dependency modeling, the data were extended by lagged features, ranging to 5 steps in the past.

When it comes to HTM models, the preprocessing was minimal. No initial data filtering or augmentation was performed. The only transformation included shifting usage values by adding a set amount, different for each SKU, to eliminate negative values. To ensure a proper forecast, the same value was later subtracted from the predictions. As per the model requirements, the data were then binary encoded, using a RDSE encoder for the raw usage data, and a default date encoder, set to encode only the seasonal portion of the date information. For the scalar encoder, its resolution varied, depending on the data series being encoded, and was calculated based on the minimal change between data points and the series width, understood as a difference between maximal and minimal value. After that, both portions of the encoded data were concatenated and converted into a SDR.

For the purpose of training, we separated the dataset into individual SKU subsets. Models were trained independently for each of the SKUs. As a validation set, we have separated observations corresponding to 13 last weeks of the set. This set was left out of the training process and was used solely for the purpose of evaluating models predictions. As the accuracy metric, we have chosen the root mean square error metric (RMSE). Since the SKU data are only applicable in real-word cases when aggregated per month, the predictions for the validation period were transformed as such, and RMSE was calculated between the both aggregations. This approach allows us to negate the adverse effect of minimal spatial misalignments (~1 week) between the prediction and real data when it comes to calculating RMSE.

The exact training process differed slightly between the approaches. For SARIMA models, 400 variants of parameter combinations were tested, and the one scoring best on the validation set was chosen. Both of the neural network architectures—LSTM and transformer—were trained for 100 epochs with the early stopping mechanism being implemented. Each run has been repeated 5 times, and the best fitting model, according to RMSE, was saved. Around 120 parameter variants of triple exponential smoothing options were checked, and the best combination, based on RMSE score on validation set, has been saved. When it comes to linear machine learning models, a number of candidates were tested for each of SKUs—linear regression, ridge regression, random forest, Huber regression, multi-layer perceptron, and AdaBoost regression. Each of the models was fitted on a training subset of each series, and its accuracy was tested on a validation set. The model with the best accuracy score was chosen as most appropriate to forecast the series. Due to the construction of the DFT regressor, this model did not required any optimal hyperparameters search procedure.

The HTM model being tested consisted of a standard set described in literature—spatial pooler, temporal memory, and a predictor module. During the training phase, a total set of 50 models per SKU were trained. The best performing model was chosen based on a combined accuracy metric. To ensure both, a good representation of the specific characteristics of a series, as well as its general trend, the metric was calculated as a weighted average of the RMSE calculated on a weekly granulation and of the RMSE calculated on data aggregated per month, with slightly higher weight placed on the monthly aggregate.

4 Results

The results of the analysis are presented in Table 1. As we described before, the main comparison metric was RMSE calculated between monthly aggregated data from the validation set and corresponding predictions aggregated as such. For simplicity sake, each SKU was assigned a numeric id, which is presented in the first column of the table. Subsequent columns contain scores of models as follows: Holt-Winters (H-W), SARIMA, machine learning (ML), discrete Fourier transform (DFT), transformer model (TF), long short-term memory model (LSTM), hierarchical temporal memory (HTM). The most accurate model for each SKU is highlighted in bold.

The results show that HTM models are highly competitive when it comes to forecasting a stochastic time series. In this particular case, out of 21 different raw material usages over time, HTM models were the most accurate in 8 of them. For those 8 cases, HTM models, on average, showed around 20% improvement (from 4.5% to 47.6%) when compared to the next most accurate approach. Out of the commonly used approaches, SARIMA models proved to be the most accurate with 6 out of 21 best predictions, placing second after HTM.

Was SARIMA with only 6 out of 21.

Table 1 Comparison of RMSE metrics calculated on monthly aggregated predictions, for all the commonly used approaches and HTM models

	H-W	SARIMA	ML	DFT	TF	LSTM	HTM
1	205.5	304.8	203.0	197.0	254.9	311.6	**168.3**
2	619.6	641.9	**153.6**	541.4	636.3	594.1	274.9
3	866.8	**305.2**	488.6	911.6	730.8	1200.5	793.6
4	364.8	205.6	175.8	1244.3	1154.8	871.7	**139.0**
5	87.8	**11.0**	65.3	330.4	151.4	130.5	20.3
6	202.9	**41.9**	507.6	505.5	2511.0	2257.7	1481.8
7	1065.3	571.3	709.5	1790.1	1601.1	1834.5	**457.0**
8	31.4	14.5	23.8	130.7	38.2	22.6	**13.8**
9	423.4	**242.2**	887.3	355.2	310.4	423.8	332.4
10	194.4	95.9	260.4	751.9	324.1	398.5	**22.8**
11	**519.9**	581.3	787.1	1915.0	1655.9	1305.2	587.4
12	86.0	87.1	117.6	111.7	118.4	**54.8**	73.1
13	23.3	23.5	21.2	11.6	13.0	**10.5**	21.4
14	34.1	33.3	39.0	41.3	32.7	**26.1**	27.5
15	29.9	5.2	19.7	17.5	36.2	18.4	**4.0**
16	26.9	11.2	**6.3**	98.8	110.7	72.7	21.0
17	102.6	**81.6**	153.5	194.6	199.3	463.2	85.4
18	274.8	**101.7**	230.6	1321.7	1016.3	942.7	691.8
19	26.4	16.1	27.0	46.4	22.8	23.4	**14.5**
20	87.1	59.3	65.6	392.7	197.5	104.4	**31.1**
21	**151.3**	257.4	506.3	341.1	620.3	586.0	193.2

5 Discussion and Conclusion

The main aim of this paper was to examine how the HTM model compares to other, already established forecasting methods when applied to predicting a real, highly stochastic time series. For this purpose, a set of data representing raw material usage in a food processing company was used. As a representative group of commonly used approaches, several different models were chosen, namely Holt-Winters, SARIMA, machine learning models, DFT, transformer model, and LSTM model.

For the purpose of a fair comparison, a minimal necessary amount of preprocessing was applied on the dataset for each model. The last 13 weeks of the datasets were established as a validation set on which the models predictions accuracy was compared. The HTM models proved to be the most accurate in 8 out of the 21 cases, with overall gain in accuracy around 20%, ranging from 4.5 to 47.6%. It is worth noting that the HTM models were successfully trying to model the real shape of the modeled data series, including cyclic "spikes," that would be interpreted as anomalies by other methods. When analyzed in weekly granulation, this feature of

HTM models proved to be detrimental in some cases, when measured by a RMSE metric. This happened due to prediction misalignment with the real values by an order of a single granulation unit (1 week), which in real-world applications are of little significance. That assumption was further proven, when the data were analyzed in monthly aggregation, in which the aggregated HTM forecast closely aligned with the aggregated target series.

The results of this study prove that HTM models are noise resistant and able to model even short time series. Additionally, this approach is able to represent volatile data, with changing trend and variability, as opposed to the most of statistical models. This ability is shared by artificial neural networks, but they require a longer data sample to adapt to the change and do not retain information about a long absent patterns.

When it comes to the data with no apparent patterns, simpler models were the most accurate, as they modeled only the average value of the time series, thus achieving the lowest RMSE scores.

Although the present study provides promising results, it is only preliminary, and further improvements could be possible, when applied to a wider range of data. Moreover, in this study, we assumed only a necessary level of preprocessing, but HTM models could benefit from additional data enhancing and feature engineering. This includes, extending the datasets with exogenous information, not present in this analysis.

References

1. Adhikari R, Agrawal RK (2013) An introductory study on time series modeling and forecasting. Lambert Academic Publishing, Saarbrücken, Germany
2. Ao S-I (2010) Applied time series analysis and innovative computing. In: Lecture notes in electrical engineering, vol 59
3. Wei WWS (2013) Time series analysis. In: Little TD (ed) The Oxford handbook of quantitative methods in psychology, vol 2: statistical analysis. Oxford University Press, Inc., New York
4. Clements MP, Franses PH, Swanson NR (2004) Forecasting economic and financial time-series with non-linear models. Int J Forecast 20(2):169–183
5. De Gooijer JG, Hyndman RJ (2006) 25 years of time series forecasting. Int J Forecast 22(3):443–473
6. Wang W, Yang J, Xiao J, Li S, Zhou D (2015) Face recognition based on deep learning. In: Lecture notes in computer science, pp 812–820
7. Xiao Y, Wu J, Lin Z, Zhao X (2018) A deep learning-based multi-model ensemble method for cancer prediction. Comput Methods Programs Biomed 153:1–9
8. Villacrés JF, Auat Cheein F (2020) Detection and characterization of cherries: a deep learning usability case study in Chile. Agronomy 10(6):835
9. Cui Y, Ahmad S, Hawkins J. Continuous online sequence learning with an unsupervised neural network model. Neural Comput 28(11):2474–2504
10. Ahmad S, Scheinkman L (2019) How can we be so dense? The benefits of using highly sparse representations. Numenta, Redwood City, California
11. Cui Y, Ahmad S, Hawkins J (2017) The HTM spatial pooler—A neocortical algorithm for online sparse distributed coding. Front Comput Neurosci 11

12. Chen P, Niu A, Liu D, Jiang W, Ma B (2018) Time series forecasting of temperatures using SARIMA: an example from Nanjing. In: IOP conference series: materials science and engineering, vol 394, p 052024
13. Vagropoulos SI, Chouliaras GI, Kardakos EG, Simoglou CK, Bakirtzis AG (2016) Comparison of SARIMAX, SARIMA, modified SARIMA and ANN-based models for short-term PV generation forecasting. In: 2016 IEEE international energy conference (ENERGYCON)
14. Dabral PP, Murry MZ (2017) Modelling and forecasting of rainfall time series using SARIMA. Environ Process 4(2):399–419
15. Valipour M (2015) Long-term runoff study using SARIMA and ARIMA models in the United States. Meteorol Appl 22(3):592–598
16. Out AO, Osuji GA, Opara J, Mbachu HI, Iheagwara AI (2014) Application of Sarima models in modelling and forecasting Nigeria's inflation rates. Am J Appl Math Stat 2(1):16–28
17. Choi T-M, Yu Y, Au K-F (2011) A hybrid SARIMA wavelet transform method for sales forecasting. Decision Support Syst 51(1):130–140
18. Billah B, King ML, Snyder RD, Koehler AB (2006) Exponential smoothing model selection for forecasting. Int J Forecast 22(2):239–247
19. Chatfield C (1978) The Holt-Winters forecasting procedure. Appl Stat 27(3):264
20. Gardner ES, Dannenbring DG (1980) Forecasting with exponential smoothing: some guidelines for model selection. Decision Sci 11(2):370–383
21. Ostertagová E, Ostertag O (2012) Forecasting using simple exponential smoothing method. Acta Electrotechnica et Informatica 12(3)
22. Taylor JW (2003) Short-term electricity demand forecasting using double seasonal exponential smoothing. J Oper Res Soc 54(8):799–805
23. Athanasopoulos G, de Silva A (2012) Multivariate exponential smoothing for forecasting tourist arrivals. J Travel Res 51(5):640–652
24. Bodger PS, Brooks DRD, Moutter SP (1987) Spectral decomposition of variations in electricity loading using mixed radix fast Fourier transform. In: IEE Proc C Gener Trans Distrib 134(3):197
25. Chen M-Y, Chen B-T (2014) Online fuzzy time series analysis based on entropy discretization and a fast Fourier transform. Appl Soft Comput 14:156–166
26. Liu S, Shan T, Tao R, Zhang YD, Zhang G, Zhang F, Wang Y (2014) Sparse discrete fractional Fourier transform and its applications. IEEE Trans Signal Process 62(24):6582–6595 (2014).
27. Chatfield C (1977) Some recent developments in time-series analysis. J Roy Stat Soc Ser A (Gen) 140(4):492
28. Lukhyswara P, Putranto LM, Ariananda DD (2019) Solar irradiation forecasting uses time series analysis. In: 2019 11th International conference on information technology and electrical engineering (ICITEE)
29. Lewisa BG, Herbertb RD, Bellc RD (2003) The application of Fourier analysis to forecasting the inbound call time series of a call centre
30. Pritz PJ, Perez D, Leung KK (2020) Fast-Fourier-forecasting resource utilisation in distributed systems. In: 2020 29th International conference on computer communications and networks (ICCCN)
31. Ahmed NK, Atiya AF, Gayar NE, El-Shishiny H (2010) An empirical comparison of machine learning models for time series forecasting. Econ Rev 29(5–6):594–621
32. Qian X-Y (2017) Financial series prediction: comparison between precision of time series models and machine learning methods
33. Pavlyshenko B (2019) Machine-learning models for sales time series forecasting. Data 4(1):15
34. Bontempi G, Ben Taieb S, Le Borgne Y-A (2013) Machine learning strategies for time series forecasting. In: Lecture notes in business information processing, pp 62–77
35. Lim B, Zohren S (2021) Time-series forecasting with deep learning: a survey. Philos Trans Roy Soc A: Math Phys Eng Sci 379(2194)
36. Coulibaly P, Anctil F, Bobée B (2001) Multivariate reservoir inflow forecasting using temporal neural networks. J Hydrol Eng 6(5)
37. Ho S, Xie M, Goh T (2002) A comparative study of neural network and Box-Jenkins ARIMA modeling in time series prediction. Comput Ind Eng 42(2–4):371–375

38. Tokgoz A, Unal G (2018) A RNN based time series approach for forecasting Turkish electricity load. In: 2018 26th Signal processing and communications applications conference (SIU)
39. Tsai Y-T, Zeng Y-R, Chang Y-S (2018) Air pollution forecasting using RNN with LSTM. In: 2018 IEEE 16th International conference on dependable, autonomic and secure computing, 16th International conference on pervasive intelligence and computing, 4th International conference on big data intelligence and computing and cyber science and technology congress
40. LeCun Y, Bengio Y, Hinton G (2015) Deep learning. Nature 521(7553):436–444
41. Miyajima R (2017) Deep learning triggers a new era in industrial robotics. IEEE MultiMedia 24(4):91–96
42. Manaswi NK (2018) RNN and LSTM. In: Deep learning with applications using python, 115–126
43. Vaswani A, Shazeer N, Parmar N, Uszkoreit J, Jones L, Gomez AN, Kaiser L, Polosukhin I (2017) Attention is all you need. In: Guyon I, Luxburg UV, Bengio S, Wallach H, Fergus R, Vishwanathan S, Garnett R (eds) Advances in neural information processing systems, vol 30
44. Wu N, Green B, Ben X, O'Banion S (2020) Deep transformer models for time series forecasting: the influenza prevalence case. arXiv:200108317
45. Zhou H, Zhang S, Peng J, Zhang S, Li J, Xiong H, Zhang W (2021) Informer: beyond efficient transformer for long sequence time-series forecasting. arXiv:201207436
46. Hole KJ, Ahmad S (2021) A thousand brains: toward biologically constrained AI. SN Appl Sci 3(8)
47. Hawkins J, Ahmad S, Cui Y (2017) A theory of how columns in the neocortex enable learning the structure of the world. Front Neural Circ 11
48. Wu J, Zeng W, Chen Z, Tang X-F (2016) Hierarchical temporal memory method for time-series-based anomaly detection. In: 2016 IEEE 16th international conference on data mining workshops (ICDMW)
49. Hawkins J, Ahmad S (2016) Why neurons have thousands of synapses, a theory of sequence memory in neocortex. Front Neural Circ 10
50. Ahmad S, Hawkins J (2016) How do neurons operate on sparse distributed representations? A mathematical theory of sparsity, neurons and active dendrites. arXiv:160100720

Preliminary Results on Constraint Programming and Branch & Bound Algorithms for the Cyclic Bandwidth Sum Problem

Valentina Narvaez-Teran, Eduardo Rodriguez-Tello, Frédéric Lardeux, and Gabriel Ramírez-Torres

Abstract The cyclic bandwidth sum problem (CBSP) consists in embedding a host graph into a cycle graph while minimizing the sum of cyclic distances between guest adjacent vertices embedded in the host. While the problem has been addressed by heuristic and metaheuristic methods, to the best of our knowledge, this is the first effort to apply exact methods. This work presents preliminary results on the use of constraint programming (CP) and a branch & bound (B&B) algorithm to solve the cyclic bandwidth sum problem in small graphs from commonly employed topologies. We created a CP model of the CBSP and devised two further refined versions by adding new constraints based in problem-specific knowledge. For our proposed B&B algorithm, we designed a custom criterion for search priority employing estimations of potential cost. The results provided an assessment of the pros and cons of both methodologies, with the CP approach offering a more reliable alternative in terms of solved instances, execution time, and implementation effort.

Keywords Cyclic bandwidth sum problem · Exact solution methods · Constraint programming · Branch & bound

V. Narvaez-Teran (✉) · E. Rodriguez-Tello · G. Ramírez-Torres
Cinvestav—Tamaulipas, Km. 5.5 Carretera Victoria-Soto La Marina, 87130 Victoria Tamps., Mexico
e-mail: maria.narvaez@cinvestav.mx

E. Rodriguez-Tello
e-mail: ertello@cinvestav.mx

G. Ramírez-Torres
e-mail: grtorres@cinvestav.mx

F. Lardeux
LERIA, SFR MATHSTIC, Univ Angers, 49000 Angers, France
e-mail: frederic.lardeux@univ-angers.fr

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_11

1 Introduction

The cyclic bandwidth sum problem (CBSP) is a graph embedding problem (GEP) [2] formally defined as follows. Let $G = (V, E)$ be a simple finite undirected graph (the guest) of order n, and C_n a cycle graph (the host) with vertex set $|V_H| = n$ and edge set E_H. Given an injection $\varphi : V \rightarrow V_H$, the cyclic bandwidth sum (CBS) is defined as:

$$\mathrm{CBS}(G, \varphi) = \sum_{(u,v)\in E} |\varphi(u) - \varphi(v)|_n, \tag{1}$$

where $|x|_n = \min\{\,|x|, n - |x|\,\}$ (with $1 \leq |x| \leq n - 1$) is the *cyclic distance*, and the vertex in V_H associated with vertex $u \in V$ is denoted by the label $\varphi(u)$. The CBSP consists in finding the optimal embedding φ^*, such that $\mathrm{CBS}(G, \varphi^*)$ is minimum, i.e., $\varphi^* = \arg\min_{\varphi\in\Phi}\{\mathrm{CBS}(G, \varphi)\}$ with Φ denoting the set of all possible embeddings.

The CBSP is an NP-Hard GEP [2] that arises in the simulation of network topologies for parallel computer systems, scheduling in broadcasting based networks, and compressed sensing in sensor networks [5, 6, 8]. It has been tackled with an ad hoc constructive heuristic [3] and metaheuristic algorithms [12, 14]. However, to the best of our knowledge, there is no exact methods reported to solve it.

In this paper, we explored the use of constraint programming (CP) [11] and branch & bound (B&B) [9] for solving small instances of the CBSP. We created a CP model and incrementally refined it by adding more problem-related information. Then, we compared it with our B&B algorithm, which was also designed with the CBSP in mind. These methods give us a preliminary assessment of the use of exact approaches for our problem and their potential for their improvement.

The rest of this work is organized as follows. Section 2 presents an initial CP model and two refinements. Then, our B&B algorithm is described in Sect. 3. A performance comparison for these methods is presented in Sect. 4. Finally, Sect. 5 summarizes our findings and future work.

2 Constraint Programming Modeling

CP is a useful paradigm for solving satisfiability and optimization problems by employing a declarative approach, where problems are described by models stating their characteristics. CP models are processed by solver software using efficient filtering algorithms for search space exploration, while the model serves as a guide to discard regions and to recognize optimal solutions. Models use three main types of components to describe problems: variables, domains, and constraints. The variables represent the solution to be created by exploring the specified domains, and the constraints are conditions the variables must met, including the problem's objective.

A problem is solved through its CP model by producing valid solutions, in the form of assignations of domain values to the variables, such that the constraints are not broken [13].

CP can be particularly powerful for discrete combinatorial problems, because of the finite domain character of their variables [1]. The constraint propagation is a key distinctive aspect in CP. It reduces the search space recursively, by discarding constraint breaking values from the domains of the variables and using information about those values to reduce the domain of other variables involved in the same constraint.

Once a good model is available, the CP approach is accessible and relatively easy to implement, thanks to frameworks of specialized software, providing modeling languages, interpreters, compilers, and solvers to create and process the models. Solvers implement advanced search algorithms based on trees, backtracking, and techniques from various areas, such as mathematical programming, operational research and artificial intelligence, to efficiently explore within the bounds defined by a CP model. The CP models in this work were created using Minizinc [10], an standardized modeling language that acts as an intermediary between the user and solvers.

2.1 An Initial CBSP Model

Often, the same constraint can be expressed in different ways, some of which may result more efficient. Therefore, it is key to effectively translate the features of the problem into the CP paradigm. Performance can also benefit from a certain redundancy in the constraints.

Data representation. CBSP instances consist of finite simple undirected graphs. The format representation contains the number of vertices n, the number of edges e, a 2-D array $E(1 \dots e, 1 \dots 2)$ listing the edges, where $E(i, 1)$ and $E(i, 2)$ are the endpoints of the ith edge.

Variables. The decision variables represent the labeling, such that $g(1..n)$ is an array of the labels assigned to vertices, where $g(i)'$ is the label mapping guest vertex $i \in V$ to host vertex $g(i) \in V'$.

Constraints. CBSP embeddings are bijective mappings between guest and host vertices, so the first constraint is that to each unique guest vertex corresponds to one unique host vertex as a label, such that $\forall i, j \in [1..n] \mid i < j$ with $g(i) \neq g(j)$. This constraint would be equal to a series of pairwise conjunctions stating that no pair of vertices can have the same label, in the form $g(1) \neq g(2) \wedge g(1) \neq g(3) \wedge \cdots \wedge g(1) \neq g(n) \wedge \cdots \wedge g(n-1) \neq g(n)$. Large conjunctions can be costly to compute, so many solvers implement instead customized efficient algorithms based on inferences. These algorithms can be accessed via global constraints, which are concisely express relationships among several variables. In terms of representation and reasoning, they provide a higher level of abstraction and better structure to the problem, allowing filtering algorithms to be much more specialized and efficient. Therefore, we used the global constraint $alldifferent$ [7], stating that all elements in an array must be pairwise distinct.

$$alldifferent(g) \tag{2}$$

Objective function. The cost of a solution is the sum of cyclic distances $cbs = \sum_{i=1}^{e} distance(i)$, where $distance(i)$ is the cyclic distance associated with edge i. Each cyclic distance can have a value between 1 and $d_{\max} = \lfloor n/2 \rfloor$. A cyclic distance equals the length of the shortest path between two adjacent vertices of the guest graph embedded in the host graph, expressed as $\forall i \in [1 \ldots e]$ $distance(i) = \min\{n - |g(E(i,1))|, |g(E(i,2))|\}$. The goal of the CBSP is to find the lowest cost embedding; therefore, the objective function for the model is to minimize the sum of cyclic distances.

$$minimize(cbs) \tag{3}$$

The first CBSP model is M_0, defined by the previously defined variables, and the conjunction of the constraints and the objective, $M_0 = (2) \wedge (3)$.

2.2 Refined CP Models

Breaking cyclic symmetries. Since the host topology is cyclic, different labelings can result in isomorphic embeddings under rotation and mirror symmetries. To remove those solutions from the search space, two constraints were added, ensuring that only the lexicographicaly minor of the isomorphic embeddings is computed. They state that the fist vertex must be associated with the fist label and that the label of the second vertex must be lower than the label of the last one, thus eliminating the rotation and mirror symmetries, respectively. The first refined model, M_1, results from adding these symmetry breaking constraints to the initial model, thus $M_1 = M_0 \wedge (4) \wedge (5)$.

$$g(1) = 1 \tag{4}$$

$$g(2) < g(n) \tag{5}$$

Adding upper and lower bounds. Including cost bounds can improve the performance by discarding solutions with cost outside the bounds. The data representation was modified to include two new input variables, the CBS lower bound lb and upper bound ub. These values vary according to each graph topology.[1] In the case of graph

[1] Lower and upper bounds: https://www.tamps.cinvestav.mx/ertello/cbsp.php.

topologies for which there are exact formulas to calculate the value of the optimum, both ub and lb got assigned that value. If this is not the case, the value of ub was calculated according to topology specific upper bound formulas, in the case where those exist, or the topology independent upper bound formula, otherwise. The value of lb was set as $e + 1$. Model M_2 results from adding the upper and lower bound constraints to model M_1; therefore, $M_2 = M_1 \wedge$ (6). Notice that in the case the exact value of the optimum is known, then $ub = lb$ and the constraints still hold.

$$lb \leq cbs \leq ub \tag{6}$$

3 A Branch and Bound Algorithm for the CBSP

B&B algorithms use a tree to implicitly explore a problem's search space by creating partitions of smaller subproblems. The nodes of the tree contain partially defined solutions to such subproblems. From the root of the tree, the exploration process branches promising nodes into new ones, creating partial solutions of higher order, and pruning branches that can not lead to the optimum. This narrows the search,

Algorithm 1: Branch and Bound algorithm

```
$up \leftarrow$ dfs($G$)
$Q \leftarrow$ empty priority queue
Create root solution $a$ by assigning $a(1) \leftarrow 1$
$Q.push(a)$
while $Q$ is not empty do
  $b \leftarrow Q.pop()$
  $i \leftarrow$ first unassigned node in $b$
  for $j \in$ { unassigned labels in $b$} do
    $b' \leftarrow b$
    $b'(i) \leftarrow j$
    $cost(b') \rightarrow f_p(b') + f_e(b')$
    if $cost(b') < f(up)$ then
      if all vertices in $b'$ are assigned then
        $up \leftarrow b'$
      else
        $Q.push(b')$
      end if
    else
      Discard $b'$
    end if
  end for
end while
$g \leftarrow up$
return $g$
```

discarding search space regions that do not contain the optimum [9]. Algorithm 1 shows our B&B. It begins by creating a solution to use its cost as initial upper bound. This solution is created by a greedy labeling algorithm based on a depth first search visit of the vertices of G, starting randomly.

The tree's root is a partially defined solution of order one, with the first label assigned to the first vertex. This solution is inserted in a priority queue to keep track of the exploration, which ends when the queue is empty. When a partial solution b is extracted from the queue, the branching process creates new nodes by assigning the unused labels to the first unlabeled vertex in b. This produces $n - o(b)$ new partially defined solutions, where n is the number of vertices and $o(b)$ is the order of b. A new solution b' is evaluated to decide if it will be further explored or discarded. Its cost $cost(b')$ is the sum of a partial CBS $f_p(b')$ given by the defined part of the solution, and a potential CBS $f_e(b')$, given by the undefined one. The partial cost is the CBS for the assigned edges, i.e., edges that have labels assigned to both endpoints. The potential CBS is a best-case estimation where all the unassigned edges have cyclic distance equal to one. A partial solution b' is discarded if the sum of partial and estimated CBS is greater than the CBS of the current upper bound solution up. If the sum is instead lower, and b' is fully defined (its order is n), then b' is better than the current upper bound solution up. Therefore, b' replaces up. Otherwise, b' cannot be discarded, so it enters the queue.

The priority queue sets the exploration order using a combination of partial solution's order, partial cost, and a more elaborated estimation of potential cost. Order is prioritized before potential cost to produce completed solutions as soon as possible. Partial solutions of equal order are untied by the sum of their partial CBS and estimation $f_b(b')$. The later is an heuristic estimation calculating the potential cost of assigning the most suitable available label to one of the endpoints of the first found edge that already has a labeled endpoint.

4 Experimental Results

We tested 30 graphs from diverse topologies commonly employed in the CBSP literature. Experiments were ran in a computer with an Intel® Core™ i7-8750H CPU at 2.20 GHz and 8 GB in RAM and 3600 s (1 h) as time limit. Our CP models were created and solved using Minizinc [10], while the B&B method was coded C++. Table 1 list the results, comparing the best solution cost and the total execution time for the algorithms. It also includes the order, size, and density of the graphs. Instances are considered solved only if the execution finished before the time limit was reached, having produced an optimum (marked in bold). Blank cells mean there was not any solution reported.

Model M_0 solved the smallest number of instances and it took the largest amount of computing time. Adding symmetry breaking constraints in the refined model M_1 was helpful to narrow the search, allowing it to solve five more instances than to the initial model M_0. It also reduced the execution time for instances previously solved

Table 1 Performance comparison of the original CP model M_0, the refined versions M_1 and M_2, as well as the branch & bound algorithm

							M_0		M_1		M_2		B&B	
Graph	$\|V\|$	$\|E\|$	den.	Op^*	lb	ub	$Best$	T	$Best$	T	$Best$	T	$Best$	T
path25	25	24	0.08	24			**24**	0.38	**24**	0.50	**24**	0.41	**24**	0.01
path30	30	29	0.07	29			**29**	0.41	**29**	0.51	**29**	0.39	**29**	0.01
path40	40	39	0.05	39			**39**	0.45	**39**	0.55	**39**	0.37	**39**	0.01
cycle25	25	25	0.08	25			**25**	0.35	**25**	0.61	**25**	0.43	**25**	0.01
cycle30	30	30	0.07	30			**30**	0.31	**30**	0.69	**30**	0.41	**30**	0.01
cycle40	40	40	0.05	40			**40**	0.41	**40**	1.81	**40**	0.45	**40**	0.01
wheel25	25	48	0.16	181			181	1hr	181	1hr	**181**	0.39		
wheel30	30	58	0.13	255			255	1hr	255	1hr	**255**	0.40		
wheel40	40	78	0.10	440			440	1hr	440	1hr	**440**	0.44		
cycleP25-2	25	50	0.17	75			**75**	819.80	**75**	15.36	**75**	0.43	**75**	27.63
cycleP30-2	30	60	0.14	90			90	1hr	**90**	231.94	**90**	0.48	**90**	423.72
cycleP40-2	40	80	0.10	120			120	1hr	120	1hr	**120**	0.51		
cycleP25-3	25	75	0.25	150			150	1hr	150	1hr	**150**	0.36	150	1hr
cycleP30-3	30	90	0.21	180			180	1hr	180	1hr	**180**	0.33	180	1hr
cycleP40-3	40	120	0.15	240			240	-	240	1hr	**240**	0.3	240	1hr
c4c3	12	24	0.36		25	52	**52**	298.18	**52**	15.08	**52**	24.31	**52**	9.33
p4p3	12	17	0.26		18	36	**29**	5.94	**29**	1.14	**29**	0.90	**29**	0.13
p4p4	16	24	0.20		25	60	**44**	876.02	**44**	70.92	**44**	51.85	**44**	17.73
p5p3	15	22	0.21		23	48	**42**	267.00	**42**	31.89	**42**	29.24	**42**	9.88
p6c3	18	33	0.22		34	123	69	1hr	**69**	2148.73	**69**	2180.70	**69**	504.16
p6p3	18	27	0.18		28	60	55	1hr	**55**	3369.98	**55**	1560.77	**55**	426.58
p3c4	12	20	0.30		21	44	**40**	54.55	**40**	5.89	**40**	2.95	**40**	1.67
p3c5	15	25	0.24		26	55	55	1hr	**55**	936.39	**55**	577.85	**55**	287.31
p4c3	12	21	0.32		22	57	**43**	65.34	**43**	5.00	**43**	4.02	**43**	2.08
p4c4	16	28	0.23		29	76	64	1hr	**64**	2458.22	**64**	2558.77	**64**	881.27
p5c3	15	27	0.26		28	87	**56**	1900.63	**56**	156.42	**56**	101.53	**56**	35.63
c3k4	12	30	0.45		31	88	**72**	1058.78	**72**	76.63	**72**	42.17	**72**	29.69
p3k4	12	26	0.39		27	80	**58**	243.11	**58**	18.12	**58**	16.18	**58**	6.19
rand10-7	10	32	0.71		33	88	**51**	19.81	**51**	1.37	**77**	2.61	**77**	1.39
rand10-9	10	41	0.91		42	113	**90**	78.99	**90**	3.54	**106**	4.88	**106**	1.70

by model M_0. The constraints for upper and lower bounds, added in the the second refined model M_2, helped it achieve further improvements in performance. Model M_2 was successful with all the graphs solved by model M_1, plus seven more. Model M_2 was the only method able to consistently solve wheel graphs, even when compared to the B&B algorithm. The performance of the later was almost comparable to model M_2, being faster in a couple of cases. However, it was not capable of solving all the considered graphs. It did not produced any solution for the wheel graphs of order larger than $n = 15$ or the power of cycle graph *cycleP40-2*. The solutions that the B&B produced for instances *cycleP25-3*, *cycleP30-3*, and *cycleP40-3* can be confirmed as optimal by comparing them with the results of model M_2, but the B&B could not demonstrate this by itself, since its execution did not finished before the maximum set time. While the B&B was, in some cases, faster than the CP models to provide an optimal result, its inability to solve several of the instances makes the CP approach with model M_2 overall more successful.

The results allowed us to evaluate the gap between the theoretical upper bound values and the optimums. For instance belonging to the Cartesian product topology, the theoretical upper bounds known were larger than the optimum by an average of 17.25%. For other instances with unknown optimal value, like the last two instances in Table 1, the gap respect to the upper bound formula for any graph was 9.34% in average.

We consider that there is still room for improving the results. CP's performance responded very positively to relatively small changes in the construction of the models that added knowledge of the problem, such as the lower and upper bounds. Therefore, further refining the models by adding more information related to the problem in the form of constraints could further help to solve a broader variety of larger instances in fewer time. It may be possible to improve the B&B performance as well; however, the CP approach offers the advantage of being easier to implement, in the sense that it does not require the micromanagement of the search exploration.

5 Conclusions

This work explored CP and a customized B&B algorithm as means to solve the CBSP. To the best of our knowledge, this work is the first proposal and performance comparison of exact methods for the CBSP.

The CP and B&B approaches were tested on a set of topologically diverse standard instances of order $n \leq 40$, with one hour as the execution time limit. When comparing the results, the CP approach was proven to be more reliable than the B&B algorithm, as shown by model M_2 solving the largest number of instances across all the included topologies. In total, the CP models and the B&B algorithm produced optimal solutions for 30 problem instances. These optimal cost values allowed us to evaluate the gap respect to the theoretical upper bounds for the Cartesian product topology [4], finding that, the known upper bound values were in average 17.25% larger than the optimal cost.

Considering the results obtained, it is worth exploring the possibility of further refinements of the CP models, specially by adding new constraints using tighter estimations for the cost bounds. It is also desirable to test more graph topologies with unknown upper bound values.

References

1. Bockmayr A, Hooker JN (2005) Constraint programming. In: Discrete optimization, Handbooks in operations research and management science, vol 12. Elsevier, pp. 559–600. https://doi.org/10.1016/S0927-0507(05)12010-6
2. Chung FRK (1988) Labelings of graphs. In: Beineke LW, Wilson RJ (eds) Selected topics in graph theory, vol 3, chap 7. Academic Press, pp 151–168
3. Hamon R, Borgnat P, Flandrin P, Robardet C (2016) Relabelling vertices according to the network structure by minimizing the cyclic bandwidth sum. J Complex Netw 4(4):534–560. https://doi.org/10.1093/comnet/cnw006
4. Jianxiu H (2001) Cyclic bandwidth sum of graphs. Appl Math J Chin Univ 16(2):115–121. https://doi.org/10.1007/s11766-001-0016-0
5. Li Y, Liang Y (2018) Compressed sensing in multi-hop large-scale wireless sensor networks based on routing topology tomography. IEEE Access. https://doi.org/10.1109/ACCESS.2018.2834550
6. Liberatore V (2002) Multicast scheduling for list requests. In: Proceedings of the 21st annual joint conference of the IEEE computer and communications societies, vol 2. IEEE, pp 1129–1137. https://doi.org/10.1109/INFCOM.2002.1019361
7. Mehlhorn K, Thiel S (2000) Faster algorithms for bound-consistency of the sortedness and the alldifferent constraint. In: Dechter R (ed) Principles and practice of constraint programming—CP 2000. Springer, Berlin Heidelberg, Berlin, Heidelberg, pp 306–319
8. Monien B, Sudborough IH (1990) Embedding one interconnection network in another, vol 7. Springer, pp 257–282. https://doi.org/10.1007/978-3-7091-9076-0_13
9. Morrison DR, Jacobson SH, Sauppe JJ, Sewell EC (2016) Branch-and-bound algorithms: a survey of recent advances in searching, branching, and pruning. Discr Optim 19:79–102. https://doi.org/10.1016/j.disopt.2016.01.005
10. Nethercote N, Stuckey PJ, Becket R, Brand S, Duck GJ, Tack G (2007) Minizinc: towards a standard CP modelling language. In: Bessière C (ed) Principles and practice of constraint programming—CP 2007. Springer, Berlin Heidelberg, Berlin, Heidelberg, pp 529–543
11. Pesant G, Gendreau M (1999) A constraint programming framework for local search methods. J Heurist 5(3):255–279. https://doi.org/10.1023/A:1009694016861
12. Rodriguez-Tello E, Narvaez-Teran V, Lardeux F (2019) Dynamic multi-armed bandit algorithm for the cyclic bandwidth sum problem. IEEE Access 7:40258–40270. https://doi.org/10.1109/ACCESS.2019.2906840
13. Rossi F, van Beek P, Walsh T (eds) (2006) Handbook of constraint programming, 1st edn. Elsevier Science
14. Satsangi D, Srivastava K, Gursaran (2012) General variable neighbourhood search for cyclic bandwidth sum minimization problem. In: Proceedings of the students conference on engineering and systems. IEEE Press, pp 1–6. https://doi.org/10.1109/SCES.2012.6199079

Analysis of Vulnerability Trends and Attacks in OT Systems

Sandeep Gogineni Ravindrababu and Jim Alves-Foss

Abstract For operational technology (OT) systems, security has been given an high priority in recent years after specific cyber-incidents targeting them. Earlier, these systems were focused mainly on reliability, and at present, security is also considered as an important factor to avoid production damage and financial losses. To improve the security in industrial systems, it is necessary to understand the flaws and provide countermeasures. In this paper, we focus on the cyber-incidents reported in Common Vulnerability Exposure (CVE) database on OT sub-systems like smart grids, Supervisory Control and Data Acquisition (SCADA) systems, embedded devices, and Programmable Logic Controllers (PLCs). We summarize the possible attacks on each of these sub-systems to gain broader insight of vulnerabilities present in them and use CVE database to enumerate trends.

Keywords Operational technology systems, Industrial control systems, SCADA, Embedded, PLCs

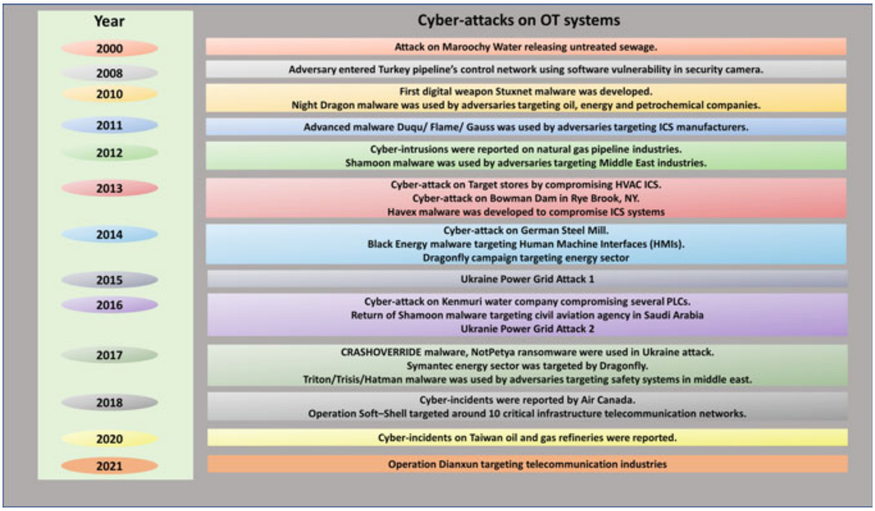
1 Introduction

Operational technology (OT) systems are computing systems that can manage industrial operations which monitor or control physical devices. Systems like oil and gas monitoring, power consumption on electricity grids, hydropower plant management fall in this category. OT systems process operational data and use various technologies for hardware design. Standard protocols used by OT systems are DNP3, MODBUS, and Profibus. The standalone nature of OT systems has diminished over the years due to the integration with corporate networks. This integration provides dynamic

S. G. Ravindrababu (✉) · J. Alves-Foss
Center for Secure and Dependable Systems, University of Idaho, 875 Perimeter Dr. MS 1008, Moscow, ID 83844-1008, USA
e-mail: sandeepg@uidaho.edu

J. Alves-Foss
e-mail: jimaf@uidaho.edu

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_12



Year	Cyber-attacks on OT systems
2000	Attack on Maroochy Water releasing untreated sewage.
2008	Adversary entered Turkey pipeline's control network using software vulnerability in security camera.
2010	First digital weapon Stuxnet malware was developed. Night Dragon malware was used by adversaries targeting oil, energy and petrochemical companies.
2011	Advanced malware Duqu/ Flame/ Gauss was used by adversaries targeting ICS manufacturers.
2012	Cyber-intrusions were reported on natural gas pipeline industries. Shamoon malware was used by adversaries targeting Middle East industries.
2013	Cyber-attack on Target stores by compromising HVAC ICS. Cyber-attack on Bowman Dam in Rye Brook, NY. Havex malware was developed to compromise ICS systems
2014	Cyber-attack on German Steel Mill. Black Energy malware targeting Human Machine Interfaces (HMIs). Dragonfly campaign targeting energy sector
2015	Ukraine Power Grid Attack 1
2016	Cyber-attack on Kenmuri water company compromising several PLCs. Return of Shamoon malware targeting civil aviation agency in Saudi Arabia Ukranie Power Grid Attack 2
2017	CRASHOVERRIDE malware, NotPetya ransomware were used in Ukraine attack. Symantec energy sector was targeted by Dragonfly. Triton/Trisis/Hatman malware was used by adversaries targeting safety systems in middle east.
2018	Cyber-incidents were reported by Air Canada. Operation Soft–Shell targeted around 10 critical infrastructure telecommunication networks.
2020	Cyber-incidents on Taiwan oil and gas refineries were reported.
2021	Operation Dianxun targeting telecommunication industries

Fig. 1 Cyber-attacks on operational technology systems

feedback for network operators to respond in real time, consequently reducing the security. Industrial control system (ICS), supervisory acquisition and data control systems (SCADA), control systems, embedded systems, smart grid systems, and power systems are all part of OT systems.

The evolution of OT systems from isolated to highly interconnected networks has resulted in a rise in computer network-based threats [11]. Several significant cyber-incidents on OT systems were listed by Hemsley et al. [15]. Figure 1 depicts the list of cyber-attacks on OT systems from the year 2000 to present. These incidents on critical and safety infrastructure have caused huge financial losses to industries and government. Vulnerabilities that were reported in Common Vulnerabilities and Exposures (CVE) database or shown in Fig. 2. Understanding the causes of these vulnerabilities and to mitigate them is very much important to secure OT systems. The key objective of this paper is to show how cyber-incidents reported on OT systems have evolved over time in the CVE database. Smart grid power systems, SCADA systems, embedded systems, PLCs, and RTUs are the primary areas of interest for us. The vulnerability trends and attacks on these systems are presented in the following sections, which will help in getting a broader knowledge of the present security mechanisms available in these systems.

2 Smart Grid Power systems

Smart grid power systems have enhanced the reliability and efficiency of supplying electricity through broadband and distribution, resulting in a cost-effective approach for power infrastructures, which impact economic stability and development of power

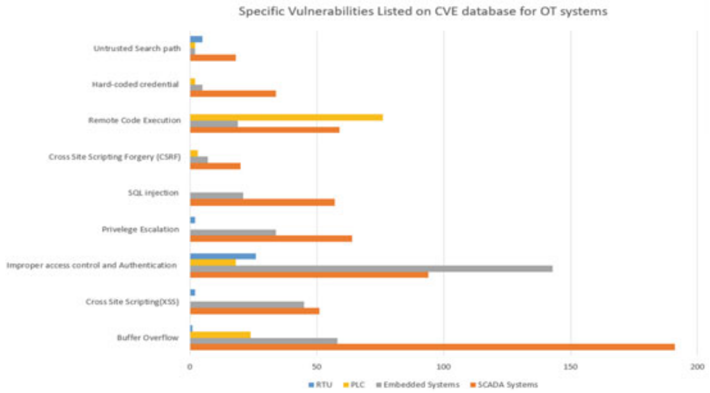


Fig. 2 Vulnerabilities reported on operational technology systems

grids. Because of improvements in distributed intelligence technologies, smart grid power systems are deemed vital in terms of economy and security. However, these solutions do not enable sufficient security enforcement, resulting in new vulnerabilities in power networks, making them vulnerable to a variety of cyber-physical attacks. E-ISAC describes one such attack in detail [5].

In smart grid power systems, there are two key components to security: Both physical and cyber security are important [20]. Physical security aims to mitigate the effects of natural disasters and other physical attacks on power systems, as well as preventing catastrophic blackouts. Cyber security aims to address the flaws introduced by the convergence of physical and cyber systems. Cyber-attacks were previously thought to be incapable of posing a threat to the security of industrial operations. But, they have caused numerous security issues in recent years and have become a major concern for both users and clients of industrial control systems [10]. Smart grid power systems add new features and capabilities to traditional power networking, making it more complicated and prone to many forms of attacks. These flaws allow attackers to get an easy access to enter the network. In 2016, four cyber-incidents were recorded on smart grids, according to the CVE database. There are a number of other events involving smart grids that aren't made public due to security concerns. Several researchers have identified the flaws in these systems, which are briefly discussed in [3] and include the following:

– Customer security.
– The number of devices(IEDs) has increased.
– Physical security.
– Between power devices, there are no trust mechanisms in place.
– Information technology (IT) protocols and industrial control system (ICS) protocols have interoperability difficulties.

Hahn et al. [14] outlined attacks like CPU exhaustion are carried out on the application layer based on these vulnerabilities. Data flooding and buffer overflow attacks were used against the network and transport layers, while man-in-the-middle attacks were used against the MAC layer and physical layer. Jamming attacks were used against the availability of smart grids and power systems. Denial-of-service (DoS) attacks can be launched against the smart grid topology, preventing operators from making proper decisions.

The specific attacks on smart grid power systems described [4, 22, 26, 32, 33] are as follows:

Load-Altering attacks attempt to manipulate or change particular load types that are available via the Internet in order to cause grid damage by causing circuit overflow or disrupting the power supply and demand balance.

Denial-of-Service An adversary disrupts some or all of the remote control system components in a smart grid attack.

Random attack An adversary conducts random attacks in order to take down the central system's detection mechanism.

False Data Injection attacks The attacker is aware of the system model, including parameters that enable control of a subset of sensors, and transmits fraudulent inputs to the main system.

Load Redistribution attack Under the logical assumption that the control center executes practical corrective steps to minimize the operation cost based on the false state estimate outcome, and attempts are made to maximize the system operation cost while targeting resource limitations.

Economic attack An adversary plans to purchase virtual power at the lower-cost node and sell it at a higher price.

Energy Deceiving An attacker can introduce falsified energy information or forged connection state information into the energy request and send response messages between nodes in this attack.

Open-loop Dynamic Load Altering An adversary tries to control vulnerable load without monitoring grid conditions, leading the grid to be impacted while the attack is being carried out.

Closed-loop Dynamic Load Altering An adversary continuously analyzes grid circumstances by hacking into a power system monitor infrastructure in order to influence the trajectory on the target load buses dependent on grid operational conditions.

Sphear Phishing is a type of cyber-attack that uses social engineering tactics to penetrate systems and networks to obtain information. A phishing email is intended to elicit a response from the receiver, such as opening an attachment or clicking on a link. The recipient may download malware or be routed to a website that requests sensitive information, such as login credentials and bank account details.

Credential Theft is a type of attack in which an opponent seeks to obtain sensitive information such as login credentials.

Data Exfiltration is an attack in which an adversary discovers hosts and devices and designs an attack concept to create a power outage in order to exfiltrate the essential information.

VPN Access An adversary hunts for existing point-to-point VPN installations on trusted third-party networks or through remote support staff connections with split tunneling enabled in this type of attack.

For the attacks mentioned above, researchers have proposed countermeasures as follows:

- Metke et al. [24] proposed countermeasures for cyber-attacks by introducing mechanisms like PKI standards, automated trust anchor security, certificate attributes, smart grid PKI tools, and trusted computing.
- Manandhar et al. [22] described a mathematical model and designed a robust framework that uses the Kalman filter with X2 detector and Euclidean detector to detect the denial-of-service (DoS) attack, random attack, and false data-injection attack.
- Electricity Information Sharing and Analysis Center (E-ISAC) has mentioned how to overcome the power system's vulnerabilities based on the attack on the Ukrainian grid [5].
- Liang et al. [20] presented strategies for preventing against economic, load distribution, and energy deceiving attacks, like protecting a set of necessary measures and PMU-based protection systems.

These mitigation methods are not yet universally accepted because of their shortcomings in terms of performance, cost, and reliability factors. Many more potential vulnerabilities are likely in the future as current technology advances. Hence, it is necessary to understand the vulnerabilities and attacks of the reported incidents in order to develop reliable and secure power infrastructures.

3 SCADA Systems

SCADA systems are typically used to monitor, gather, and process real-time data or operational data to perform specific industrial organizations operations. SCADA system consists of components like PLCs, remote terminal units (RTUs), human–machine interface (HMI), end-devices, control servers, and sensors. These components communicate internally to process data and network administrators analyze the processed data to make meaningful decisions. Earlier, the traditional SCADA system goal was to perform reliable operations from isolated locations using data historians or other proprietary technologies to handle data. This would make the process operations complicated and inefficient. Modern SCADA system solves this problem by leveraging with information technology (IT). This integration has reduced the gap between IT and SCADA systems. Modern SCADA systems enable remote access to real-time data through the Internet. As a result, SCADA networks interconnection and remote accessibility have risen, rendering them vulnerable to cyber-attacks.

Since 2007, 948 instances have been recorded in the CVE database, according to the CVE organization. The number of vulnerability incidents reported on SCADA systems each year is depicted in Fig. 3. The number of reported events

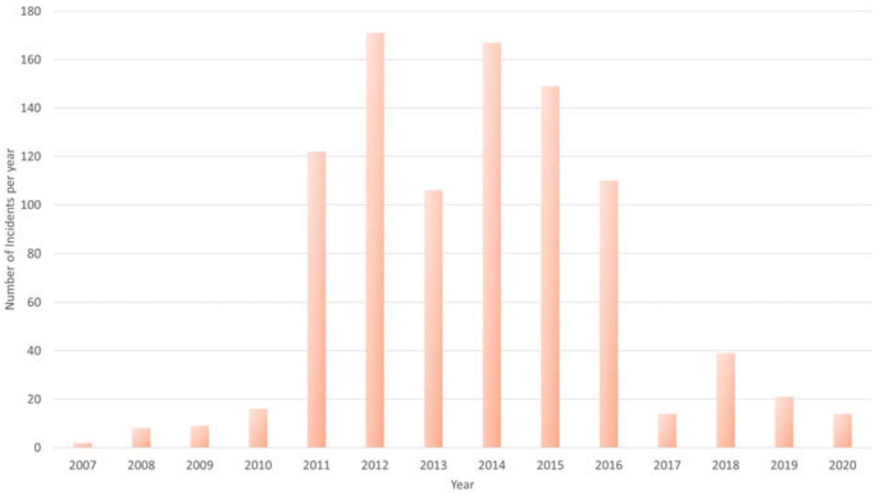


Fig. 3 SCADA system vulnerabilities reported in CVE database

peaked between 2011 and 2016, then declined in subsequent years. Based on the CVE database, the graph represents the analysis to the best of our knowledge. The vulnerabilities like buffer overflow, cross-site scripting(XSS), improper access control and authentication, privilege escalation, SQL injection, cross-site scripting forgery(CSRF), remote code execution, hard-coded credential, and untrusted search path were found in these incidents.

RTUs are integral part of SCADA systems which monitors field data and sends to SCADA control servers. There are specific incidents which were reported against RTUs in CVE database. Figure 4 depicts the number of incidents reported on RTUs. 43 incidents were reported in the CVE database on RTUs from 2010 to 2020, and maximum number of incidents were reported during the years 2018 to 2020. From the two figures Figs. 3 and 4, we can see that incidents reported on SCADA systems from 2018 to 2020 were mostly based on RTUs. Interdependency between SCADA components will be one of the important aspects that should be considered in future, and it is necessary to develop countermeasures for SCADA internal components like RTUs and PLCs.

Based on these vulnerabilities, the possible attacks on the SCADA system [7, 8, 13, 18, 27, 31] are as follows:

RADIUS Remote authentication dial-in user service DoS attack causes damage by limiting or denying access to its resources by denying the service to authorized users.

ICT Worm Infection Worm infection occurs because of the vulnerabilities found in the software installed on SCADA servers. Worms try to replicate and spread throughout the network. Then, by closing all the network connections, it isolates the SCADA systems.

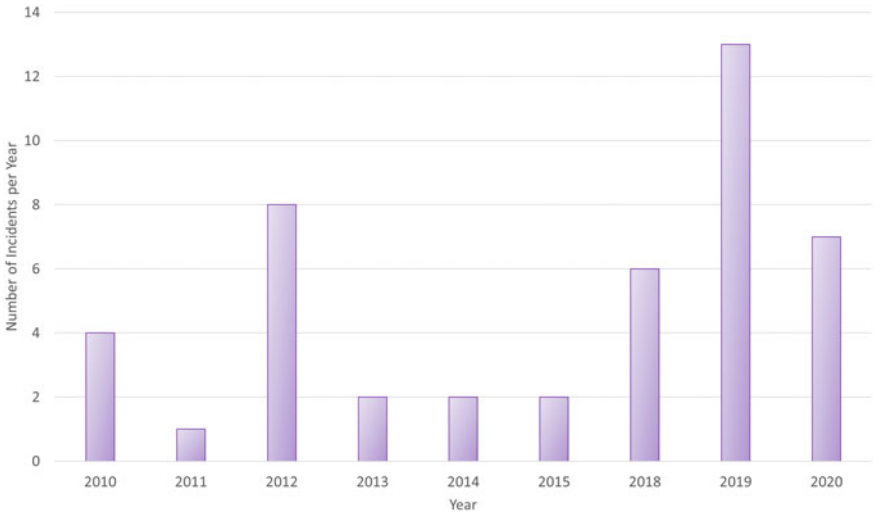


Fig. 4 RTU vulnerabilities reported in CVE database

Process Network Malware Infection attack is carried out by injecting the worm into the process network like RTUs, communicating using protocols like MODBUS or DNP3. Worms carry malware code in the payload by spreading themselves using resource hosts and executing malicious code on SCADA systems.

Phishing attack in SCADA systems is carried out by creating a fake website with a malicious code. This makes the user believe that they are connected to the legitimate website. When entered with their credentials, the adversary steals the credentials to get the SCADA system's direct access.

War Dialing Scanning attack executes the scripts on the surrounding numbers to detect potential connections once the main phone number is determined. Then the subsequent attacks are performed to penetrate into the SCADA control server.

Traffic Sniffing is used to capture the packets traversing within the network through a network analyzer.

Password Cracking is a software program that repeatedly tries to guess a password to gain unauthorized access to a network. An adversary can also use brute force or dictionary techniques to crack the password.

Warm Restart is a type of attack in which an instruction is delivered from the master controller to the PLC, compelling it to reboot right away. Warm restart is a type of DoS attack that happens on the DNP3 protocol. Multiple WarmRestart orders cause the PLC to go into a state of shutdown, resulting in a DoS.

Man-in-the-Middle attack Obtaining unauthorized access to data is the first step. The communication between the human–machine interface (HMI) and the MODBUS server is then faked, allowing attackers to send attacks to either device and then transmit busy exceptions to the HMI.

TCP SYN Flooding attack On the target device, it establishes a number of connections. It allows the system to distribute resources to each connection by leaving the connections open. The target resources are exhausted as a result of sending repeated SYN packets, forcing the system to shut down.

TCP ACK Flooding attack This is accomplished by sending numerous TCP packets with ACK enabled. The ACK packets signal that the data has been received by the target system. An adversary who does this repeatedly can bring the system to a halt.

Buffer Flooding attack By sending several events to a device that temporarily buffers SCADA data before retrieving it in the control station, an attacker can launch a buffer flooding attack. This reduces the buffering of critical warnings from approved devices, reducing the situational awareness of the control station.

Integrity attack is accomplished by delivering incorrect inputs to other devices in SCADA systems, causing data corruption.

Reconnaissance attack is used to collect information about the control system's network, map the network architecture, and identify device attributes such as the manufacturer, model number, supported network protocols, system address, and system memory, e.g., using technologies such as port scanning to find vulnerable ports.

Response injection attack take three forms: First, response injection attacks occur from the control of a PLC or RTU, as well as network endpoints, which are servers that answer to network client inquiries. Second, during the transmission from server to client, a response injection attack captures network packets and modifies their contents. Finally, response injections can be designed and sent over the network by a third-party device. Because ICS network protocols lack authentication measures to check packet origin, attackers can capture, change, and send answer packets, resulting in these attacks.

Command Injection attack injects false control and configuration commands into a control system.

Format String attack is performed against user data to compromise the root privilege account without inserting any external code.

Spoofing attack is carried out by jamming the devices across the network through interference with the device radiofrequency.

Replay attack is carried out by transmitting the malicious packets repeatedly.

Destroying a Node attack is caused by a lack of physical access security, which makes it easier for an attacker to destroy nodes or devices, particularly in sensor networks.

Environment Tampering By tampering with the sensor readings in the deployment zone, an attacker can alter the results.

Cryptanalysis attack refers to the technique of converting encrypted data into plain text without knowing how encryption works.

Exploit attack An attacker becomes accustomed to the system's vulnerabilities and launches an attack based on those vulnerabilities.

Sybil attack In this attack, a malicious device impersonates other authorized devices across the network by pretending to have several identities. This attack is carried out in sensor networks.

Replication attack Here, an attacker attempts to add one or more devices with the same name as current device.

Routing attack decreases the availability of the system as the attacker tries to create false routes.

Time Synchronization Attack Sensor networks using SCADA components rely on synchronization to perform correctly using time-synchronized protocols. Attack on these protocols results in out-of-sync between devices.

Slander attack This attack can cause each device to accuse the other if misbehavior occurs across the network. This is possible to detect if there is a implementation of distributed detection mechanism.

For the attacks mentioned above, researchers have proposed countermeasures as follows:

– Fovino et al. [28] have proposed mitigation strategies for RADIUS, ICT Worm infection, process network malware infection, phishing attacks, and DNS poisoning attacks, through the process of filtering and monitoring, and by specifying rules for TCP/IP and SCADA protocols.
– Three steps for intrusion detection were developed and proposed by Cheung et al. [8] for model-based intrusion detection.
– Vulnerability assessment framework consists of three levels—system vulnerability, scenario vulnerability, and access point vulnerability—to detect attacks like directed attacks and intelligent attacks, which is presented by Ten et al. [31].
– Mallouhi et al.[21] developed a module with a 100% detection rate to detect TCP protocol attacks (TCP SYN, TCP ACK, man-in-the-middle) with low false-positive alerts.
– Jin et al. [17] proposed to use a rule-based policy approach to overcome the Buffer-overflow attacks.
– Giani et al. [13] have developed mathematical and computational models for the interaction between the physical and infrastructure processes to overcome Integrity attacks in SCADA systems.

The preceding solutions are limited to a specific SCADA architecture testbed and therefore cannot be generalized. With the advancement of modern SCADA systems, many more new vulnerabilities are expected in the future. Therefore, it is essential to analyze vulnerability trends, sources of those vulnerabilities, and distinct attacks in order to create a secure and resilient SCADA system.

4 Embedded and Firmware systems

Advancement in hardware devices and communication technology has led to an increase in many embedded devices in critical communication infrastructures. Embedded systems are computing systems built into an extensive network, designed for dedicated functions to interact with general-purpose systems. These systems include hardware, software, and other mechanical parts [4, 33]. The widespread use of embedded devices in the Internet of things (IoT) has resulted in OT system security breaches.

One of the many problems associated with embedded devices is firmware. Firmware is a software program that provides a control for embedded systems. They are related to permanent storage devices such as microcontrollers consisting internal storage mechanisms. Microprocessors are considered the core of electronic systems, and software through firmware can effectively use various hardware interfaces associated with them. The firmware has become the primary component of any automated method. Due to this advancement, securing this has become an essential aspect in the real world [29].

Analysis of embedded systems' vulnerabilities from CVE database is provided by Kocher et al. [19], and some of them are as follows:

– Programming Errors: Control-flow attacks like input parsing vulnerabilities lead to buffer overflow attacks. Memory management problems such as pointer exception occur because of not following coding standards while developing software programs.
– Web-Based Vulnerability: Lack of updates or patches for web applications used by embedded devices are exposed to specific attacks because of the vulnerabilities existing in the web interfaces.
– Weak Access Control or Authentication: Default or weak passwords are used. To keep passwords simple, some systems have them hard-coded. This gives people who know the password backdoor access, making it easier for attackers to get around it.
– Improper use of Cryptography: Random generators for generating cryptographic keys, as well as protocol weaknesses, have a significant influence on embedded devices.

According to vulnerabilities reported in the CVE database, since 2000, around 843 incidents have been reported. Figure 5 depicts the number of vulnerability incidents reported every year on embedded systems. Until the year 2012, there were not many incidents reported in CVE database. From the years 2013 to 2018, maximum number of incidents were reported and in the years 2019 and 2020 incidents reported were less than the year 2018. This graph depicts the importance of attack vulnerabilities, and if adequate mechanisms are not implemented, attackers will have an easy time breaking into these systems and causing damage.

The effect of these vulnerabilities causes a different type of attacks on embedded and firmware systems mentioned in [6, 9, 25, 29] are as follows:

Control Hijacking attack In this attack, an adversary attempts to redirect the regular flow of a program operating on an embedded device, resulting in the attacker's code being executed.

Reverse Engineering The method of getting sensitive information by examining the software in an embedded device is known as reverse engineering. The attacker can use this method to find code flaws such as input parsing issues.

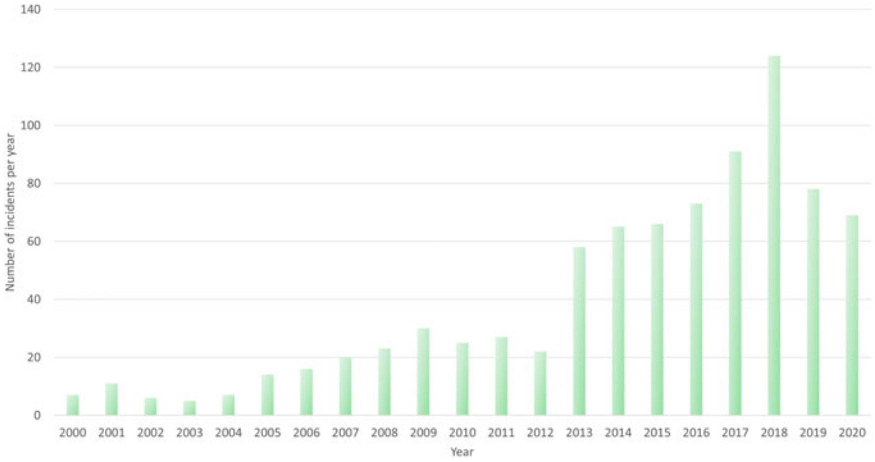


Fig. 5 Embedded device and firmware vulnerabilities reported in CVE database

Malware attack An adversary attempts to infect an embedded system with malicious software known as malware, which can change the device's behavior and have serious effects.

Brute force search attacks Because of the inadequate cryptography and authentication techniques in embedded devices, issues such as exhaustive key search may occur. Using brute force search attacks, an attacker gets around the system by logging in with random credentials.

Eavesdropping or Sniffing An attacker observes the communications transmitted and received by an embedded device in a passive attack.

Injecting Crafted Packets or Input is a technique for attacking the protocols used by embedded devices. Packet and input crafting attacks both take advantage of parsing flaws in protocol implementations or other software. Replaying previously seen packets or packet fragments is also considered a type of packet forging, which can be a good way to trigger protocol problems.

Known-key attack This occurs as a result of a flaw in the standard protocols. In the second transaction, an attacker takes the old key and supplies it twice, resulting in a known terminal key. Because the key is exclusive-or'ed with itself, they are regarded the core of all zeroes. As a result, an attacker can encrypt the PIN key using a terminal master key, allowing an ATM to validate client PINs even if the network is offline. Therefore, the attacker now has access to the PIN key, which is encrypted using the all-zero key. He can then decrypt it using his computer and calculate any customer's PIN.

Two-Time Type attack is accomplished by developing a program that maps the various key and data transformations between different essential types, computes the transitive closure, and scans the composite operations for undesired features.

Firmware Modification attack such as reprogramming the battery, affect devices with design defects, different versions of operating systems, and different instruction set architectures.

CIH Virus rewrites the BIOS firmware online, causing the BIOS firmware program to crash and fail while the systems are being loaded.

Control-Flow attack When information such as return addresses is kept with functions, an error occurs. These function variables come from unreliable sources, and there aren't enough checks in place to prevent memory corruption. An adversary can use this corruption to tamper with the control-flow information stored on the stack.

Stack-overflow attack occurs when there is too much data on the stack or when the depth of the stack is too large. In both circumstances, the stack uses up all of its memory. It overlaps with other memory portions, such as the BSS sector, posing a security, and reliability issue.

Configuration Manipulation attack allows an attacker to modify an embedded device's critical configuration parameters to force it to misbehave. These attacks are concerned with programmable devices such as PLCs, which can control the programming logic process.

For some of the attacks mentioned above, researchers have proposed countermeasures as follows:

- Hou et al. [16] proposed autotomic binary structure randomization (ABSR), which disables unnecessary features and removes the unused binary from the firmware image to overcome the firmware modification attack.
- The CIH virus was found in 1998. Numerous solutions to overcome this attack are given, like implementing fuzzy testing, behavioral analysis, and homology analysis.
- Split stack and instruction-based memory control techniques were developed by Francillon et al. [12] to overcome the control-flow and stack-overflow attacks in embedded and firmware devices.
- Memory verification and control-flow integrity techniques are used as countermeasures to overcome configuration manipulation attacks and control-flow attacks on embedded systems [1].

Preventing embedded system vulnerabilities is a formidable task since they have memory and time concerns, making security solutions difficult to apply. Understanding vulnerability trends and attacks on these systems aid in visualizing the problem at a high level and achieving solutions at the design level.

5 Programmable Logic Controller (PLC)

PLCs are real-time systems that closely monitor and control plant devices to keep the process functioning correctly. In general, PLC receives information from input devices, processes the data, and triggers outputs based on the preprogrammed parameters. This program in PLC considers as logic and executes within the control flows.

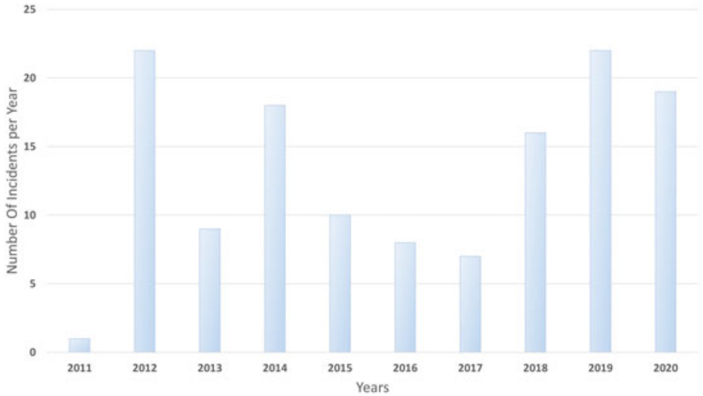


Fig. 6 PLC vulnerabilities reported in CVE database

Research works on PLCs like detection of vulnerabilities and attacks on PLCs concerning embedded systems are investigated by Abbasi et al. [1]. In this work, the author has described the different attack techniques used by an adversary to tamper the I/O operations in PLC and also showed how certain detection mechanisms implemented in PLCs can be evaded. Sandaruwan et al. [30] have revealed the vulnerabilities of PLCs through attack vectors affecting critical infrastructure, described Stuxnet attacks and proposed solutions to overcome the weaknessess in PLCs. Stephen [23] have constructed an dynamic payload, based on the process observation in control system and claimed that this process will significantly lower the attacks against PLCs. Carlos [2] have demonstrated the feasibility of power fingerprinting technology to monitor PLC and detect malicious software using Siemens S7 PLC.

According to vulnerabilities reported in the CVE database, since 2011, around 132 incidents have been reported. Figure 6 depicts the number of vulnerability incidents reported every year on PLCs. The highest number of incidents were recorded from 2012 to 2014, and then again from 2018 to 2020, indicating how susceptible the PLCs are at present.

Some of the attacks on PLC are described as follows:

Pin Control Attack consists of misusing the pin control functionalities at runtime, causing physical damage, communication block, and manipulation of reading or writing values from a device, to be a legal process. Because of the vulnerability, an attacker can modify the multiplexing registers, which leads to the disconnect of the legitimate device.

PLC Malware Stuxnet is considered to be the PLC malware, and Stuxnet intends to reach the nodes in the SCADA systems that connect to the PLC's operating the target plant MTUs. Once executing on an MTU, Stuxnet uploads its payload of static code blocking the PLC, resulting in the process to be under malicious control.

Bypass Logic attack In general, PLCs contain main memory and register memory. Register memory contains some variables associated with main logic. This register

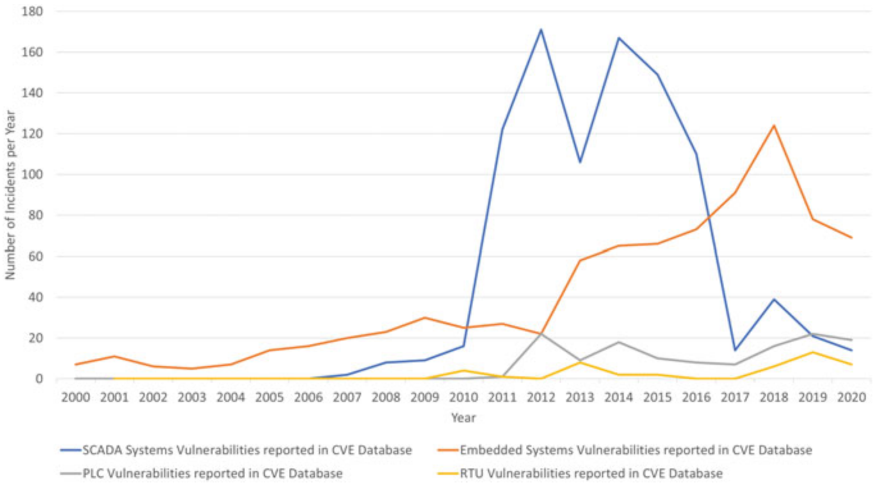


Fig. 7 Comparison of incidents reported in CVE database on SCADA, embedded, PLCs, and RTUs

memory is allowed to access by other PC's in industrial plants with read and write operations across PLC networks. When an adversary gains access to one of these machines, he can change the values arbitrarily and cause the system to collapse.

Brute-Force Output attack An operator of a PLC can aggressively manipulate the output by connecting to the PLC via a network or the Internet without any authentication. When an enemy gains access to the PLC, he can compel the output to shut off some valves and other components, resulting in disastrous consequences.

Replay attack In this attack, an adversary gets some information about PLC and uses the same information to compromise the system later.

S7 Authentication Bypass attack In this attack, an adversary can easily bypass the authentication by intercepting the valid user packet and replay that packet at later to authenticate himself. This is because of the lack of security in the protocol.

The comparison of cyber-attacks on SCADA, embedded systems, PLCs, and RTUs are given in Fig. 7. From the graph, the incidents reported on all four of the systems were at peak during the years 2010 to 2018. Even if there is a decrease in the number of incidents reported in past two years, still it is essential to analyze these trends and address the vulnerabilities of these systems.

6 Conclusion

In this paper, we have presented a list of attacks on different sub-systems of OT. We also performed analysis on the cyber-incidents reported in CVE database, to determine the trends. We believe that this list will inspire and push people to develop countermeasures to the weaknesses present in these systems. This work serves as a starting point to develop a standard set of mitigation mechanisms by bridging the gap between different OT sub-systems and helps to develop mitigation strategies for cyber-attacks to make the OT reliable and resilient. Based on this survey, we will create a testbed for each OT subsystem that integrates with software-defined networking technologies, using NIST principles, and analyze them in terms of performance, safety, security, and reliability properties.

References

1. Abbasi A (2016) Ghost in the PLC: designing an undetectable programmable logic controller rootkit via pin control attack. University of Twente Research Information, pp 1–35 (2016)
2. Aguayo Gonzalez C, Hinton A (2014) Detecting malicious software execution in programmable logic controllers using power fingerprinting. Tech. Rep. (2014)
3. Aloul F, Al-Ali AR, Al-Dalky R, Al-Mardini M, El-Hajj W (2012) Smart grid security: threats, vulnerabilities and solutions. Int J Smart Grid Clean Energy
4. Amini S, Pasqualetti F, Mohsenian-Rad H (2018) Dynamic load altering attacks against power system stability: attack models and protection schemes. IEEE Trans Smart Grid 9(4):2862–2872
5. Analysis of the cyber attack on the Ukrainian power grid (2016)
6. Bond M, Anderson R (2001) API-level attacks on embedded systems. Computer 34(10):67–75
7. Cardenas AA, Roosta T, Sastry S (2009) Rethinking security properties, threat models, and the design space in sensor networks: a case study in SCADA systems. Ad Hoc Netw 7(8):1434–1447
8. Cheung S, Dutertre B, Fong M, Lindqvist U, Skinner K, Valdes A (2006) Using model-based intrusion detection for SCADA networks, pp 209–237 (2006)
9. Cui A, Costello M, Stolfo S (2013) When firmware modifications attack: a case study of embedded exploitation
10. Cyber Security for Industrial Automation and Control Systems (IACS) Edition 2 Open Government status Open
11. Czechowski R (2016) Security policy and good practice for implementation of smart grid solutions. Przegląd Elektrotechniczny 92(3):177–181
12. Francillon A, Perito D, Castelluccia C (2009) Defending embedded systems against control flow attacks
13. Giani A, Karsai G, Roosta T, Shah A, Sinopoli B, Wiley J (2008) A testbed for secure and robust SCADA systems. ACM SIGBED Rev 5(2):1–4
14. Hahn A, Govindarasu M (2011) Cyber attack exposure evaluation framework for the smart grid. IEEE Trans Smart Grid 2(4):835–843
15. Hemsley KE, Fisher E et al (2018) History of industrial control system cyber incidents. Tech. rep., Idaho National Lab. (INL), Idaho Falls, ID (United States)
16. Hou Jb, Li T, Chang C (2017) Research for vulnerability detection of embedded system firmware. Procedia Comput Sci 107:814–818
17. Jin D, Nicol DM, Yan G (2011) An event buffer flooding attack in DNP3 controlled SCADA systems
18. Kang DJ, Lee JJ, Kim SJ, Park JH (2009) Analysis on cyber threats to SCADA systems. In: 2009 transmission & distribution conference & exposition: Asia and Pacific
19. Kocher P, Lee R, McGraw G, Raghunathan A (2004) Security as a new dimension in embedded system design. In: Proceedings of the 41st annual design automation conference, pp 753–760
20. Liang G, Zhao J, Luo F, Weller SR, Dong ZY (2017) A review of false data injection attacks against modern power systems. IEEE Trans Smart Grid 8(4):1630–1638

21. Mallouhi M, Al-Nashif Y, Cox D, Chadaga T, Hariri S (2011) A testbed for analyzing security of SCADA control systems (TASSCS). In: ISGT 2011
22. Manandhar K, Cao X, Hu F, Liu Y (2014) Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans Control Netw Syst 1(4):370–379
23. McLaughlin S (2011) On dynamic malware payloads aimed at programmable logic controllers. In: Proceedings of the 6th USENIX conference on hot topics in security, p 10
24. Metke AR, Ekl R (2010) Security technology for smart grid networks. IEEE Trans Smart Grid 1(1):99–107
25. Miller C (2011) Battery firmware hacking. Black Hat USA, pp 3–4
26. Mohsenian-Rad AH, Leon-Garcia A (2011) Distributed internet-based load altering attacks against smart power grids. IEEE Trans Smart Grid 2(4):667–674
27. Morris TH, Gao W (2013) Industrial control system cyber attacks. In: 1st international symposium for ICS & SCADA cyber security research 2013 (ICS-CSR 2013), vol 1, pp 22–29
28. Nai Fovino I, Carcano A, Masera M, Trombetta A (2009) An experimental investigation of malware attacks on SCADA systems. Int J Critical Infrastruct Protect 2(4):139–145. https://www.sciencedirect.com/science/article/pii/S1874548209000419
29. Papp D, Ma Z, Buttyan L (2015) Embedded systems security: threats, vulnerabilities, and attack taxonomy. In: 2015 13th annual conference on privacy, security and trust (PST), pp 145–152. IEEE
30. Sandaruwan GPH, Ranaweera PS, Oleshchuk VA (2013) PLC security and critical infrastructure protection. In: 2013 IEEE 8th international conference on industrial and information systems
31. Ten CW, Liu CC, Manimaran G (2008) Vulnerability assessment of cybersecurity for SCADA systems. IEEE Trans Power Syst 23(4):1836–1846
32. Yan Y, Qian Y, Sharif H, Tipper D (2012) A survey on cyber security for smart grid communications. IEEE Commun Surv Tutor 14(4):998–1010
33. Yuan Y, Li Z, Ren K (2011) Modeling load redistribution attacks in power systems. IEEE Trans Smart Grid 2(2):382–390

Simulation Model of Respiratory Sound and Technology for Separating Characteristics of Pulmonary Disease

Yiyang Luo, V. I. Lutsenko, S. M. Shulgar, and Nguyen Xuan Anh

Abstract In the process of human breathing, respiratory sounds are produced, and these sounds contain a lot of information related to the structure of the human airway. This paper uses computer and signal processing technology to collect and analyze the breath sounds to study the frequency spectrum difference between normal and abnormal respiratory sounds. Furthermore, it provides doctors/patients with a simple, quantitative, objective, intuitive, non-invasive auxiliary diagnosis tool for certain respiratory dysfunction diseases and respiratory physiology research methods.

Keywords Distribution density · Family doctor · Fast Fourier transform (FFT) · Semi-Markov process · Respiratory sounds · Spectrogram

1 Introduction

Since the invention of the first stethoscope in 1816 by Laënnec, over 200 years, people have invented a variety of new methods to help doctors confirm respiratory diseases, including:

- **electronic stethoscope**—the disadvantage is that the price is high, the audibility is poor (complex noise) so that it is difficult to correctly explain;
- **Bronchophonography**—based on the study of the frequency-amplitude characteristics of respiratory noises, however, it does not allow to determine in which part of the respiratory system the pathology is located;

Y. Luo (✉) · S. M. Shulgar
V.N. Karazin, Kharkiv National University, 4 Svobody Sq, Kharkiv 61077, Ukraine
e-mail: yiyangluo@163.com

V. I. Lutsenko
O.Ya. Usikov Institute for Radiophysics and Electronics of the National Academy of Sciences of Ukraine, 12 Academician Proskura St, Kharkiv 61085, Ukraine

N. X. Anh
Institute of Geophysics, Vietnam Academy of Science and Technology, 8-18 Hoang Quoc Viet,, Cau Giay, Hà Noi, Vietnam

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_13

- **ultrasound scanning**—in the event of pathological processes in the lungs (such as pneumonia, atelectasis or volumetric neoplasms), tissue densification and a decrease in lightness occur, which creates opportunities for the passage of ultrasound and the visualization of lesions located in the subpleural area of the lungs. The disadvantages of the method are attributed to the fact that the smallest lung tissue layer between the chest wall lung lesions does not conduct ultrasound, making the inflammation site invisible, resulting in insufficient information;
- **vibration dynamic visualization**—based on the vibration record that occurs when the air passes through the lung channel, and the subsequent computer processing of the obtained data to construct a dynamic image. Disadvantages: the sensor matrix is cumbersome and lacks the complete propagation and accurate positioning of the acoustic signal source in the lung tissue;
- **passive echolocation**—a comparative analysis of the acoustic waves of the pulmonary pattern with the standard stored in the database of the diagnostic system. After the identification of the noises, their spectral analysis is carried out and, according to the characteristics of the received noises, the coordinate of the source is calculated.

However, the most convenient and effective method is to design a new digital auscultation device connected to a computer or mobile phone based on the mechanism of a traditional stethoscope. Especially in the context of the current COVID-2019 global pandemic, due to the shortage of respiratory disease detection equipment and professional doctors, there is an urgent need for a convenient and intelligent portable small electronic stethoscope. This thesis is the theoretical foundation research carried out in this direction.

2 Theory and Equipment Basis

2.1 Semi-Markov Model of Respiratory Cycle

In previous work [1], we have proposed that the breathing process can be regarded as a semi-Markov process. Since there will be no air movement in the lungs and no respiratory sound without breathing, it is only necessary to consider the two phases of inhalation and exhalation in the breathing process as shown in Fig. 1a. Since the two states of the respiratory cycle are clear and definite, the transition of the two states of exhalation and inhalation can be described by a Markkov chain as shown in Fig. 1b.

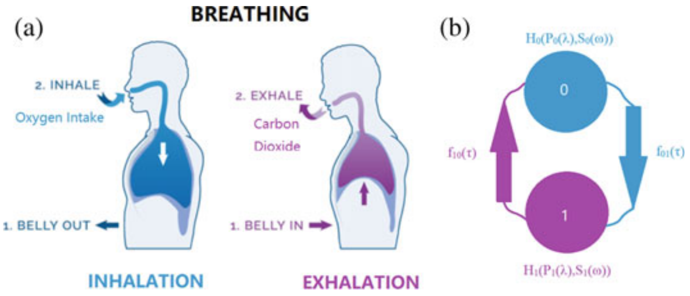


Fig. 1 **a** Schematic diagram, and **b** the Markov chain of respiration process

2.2 Generation and Classification of Respiratory Sound

In the process of exhalation and inhalation, the air flows through the trachea, bronchi to the lungs, rapid changes in air pressure and vibration of the solid tissues of the organs will generate sound waves, which are transmitted to the chest wall and neck through human tissues to form respiratory sounds. There are two types of respiratory sounds, normal, and abnormal. Normal respiratory sounds include tracheal breath sounds (TBS), vesicular breath sounds (VBS), bronchial breath sounds (BBS), and bronchovesicular breath sounds (BVBS). Abnormal breath sounds include cogwheel breath sounds, asthma sounds, and indefinite breath sounds. Abnormal breath sounds can only be heard under pathological conditions. Various breath sounds have their own characteristics, such as the position of hearing, the height, strength, length of the sound, and the time relative to exhalation and inhalation [2].

2.3 Auscultation and Quantitative Analysis of Respiratory Sound

Respiratory sounds contain a lot of information related to the structure of the airway. For example, narrowing of the airway, cavities in the lungs, edema, and the presence of foreign bodies can change the airway structure or the elasticity of the sound transmission medium, which in turn produces abnormal breathing sounds or changes the sound transmission characteristics of the respiratory system.

Stethoscopes can provide doctors with abnormal sound sources and their locations. They have been used clinically for more than 200 years. However, traditional stethoscopes have low resolution and only rely on the doctor's experience for qualitative analysis. According to the equal-loudness contour, the sensitivity of the human ear to sound is the combined effect of sound intensity and frequency, and some low-frequency, low-intensity sounds cannot be perceived by the human ear. It is difficult to distinguish artificially the changes in the respiratory sound intensity and frequency caused by the disease, so some pathological features are difficult to capture and confirm. Combined with modern digital signal processing technology, the quantitative comparison of breath sounds in the time domain and frequency domain can accurately analyze the generation mechanism of breath sounds, study the characteristics of normal/abnormal breath sounds, and further develop methods for automatic classification of respiratory diseases. This lays the theoretical foundation for the portable and convenient family doctor system.

2.4 Detection and Recording of Respiratory Sound

The collection of respiratory sounds generally uses an air-coupled electret condenser microphone, which is installed in a probe with an air cavity and pores (used to balance the atmospheric pressure). The material and specific size and structure of the probe are determined according to the selected microphone to ensure that there is no resonance and excessive attenuation in the frequency range of breathing sounds (60–1600 Hz). Respiratory sounds are usually collected in the neck and chest. The respiratory sounds in the neck are strong, and it is generally easy to find the source of abnormal sound. Respiratory sounds in the chest are mostly used to evaluate the sound transmission characteristics of the respiratory system. After being filtered and amplified, the respiratory sounds are transmitted to a mobile phone or computer for storage and analysis, as shown in Fig. 2.

3 The Statistical Characteristics of Respiratory Sound

The data processed in the experiment are respiratory sounds recorded in standard e-books. Distribution densities for different phases of respiration for healthy and

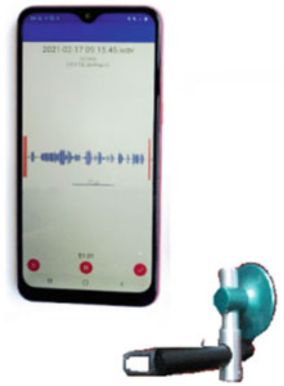


Fig. 2 A "Family Doctor" system for lung auscultation, using Samsung mobile phone and Xiaomi bluetooth headset for recording, accumulating, and transmitting data of respiratory sound

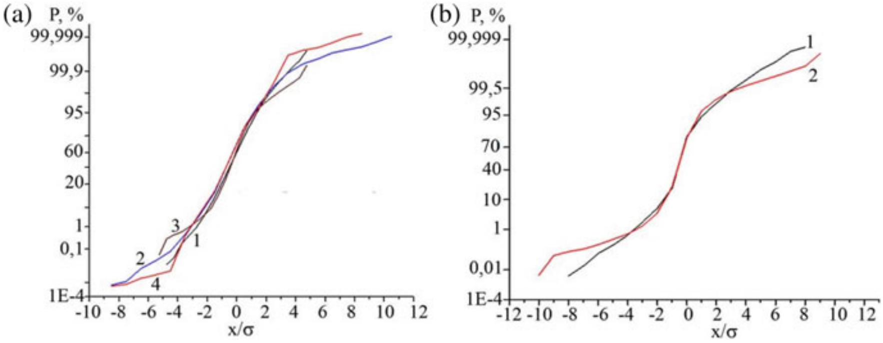


Fig. 3 Distribution densities for different phases of respiration for healthy and diseased lungs were experimentally studied (**a**), as well as for the respiration process in general (**b**): **a** 1, 3—Emissions, 2, 4—Pauses, 1, 2—Left lung, 3, 4—Right lung; **b** 1—Left lung, 2—Right lung

diseased lungs were experimentally studied—Fig. 3a, as well as for the total respiration process—Fig. 3b. They are presented in proportions of the linearized normal distribution law.

It can be seen that for the description of the distribution densities of the inhalation and exhalation phases in the range of provision levels from 01% to 99.9%, the distribution densities are satisfactorily described by the normal distribution law, and for inhalation it is better than for exhalation. For a healthy and a patient lung, the density of distribution looks approximately the same. It must be remembered that they are plotted when normalized to the root mean square (RMS) value. This means that the form of distribution functions (in coordinates normalized to the RMS value) is not a distinctive feature for recognizing pathologies of the respiratory process. In each of the phase states (inhalation or exhalation), the sounds of the breathing process are satisfactorily described by standard Gaussian models. In this case, the distribution function of the respiration process as a whole will be described by a poly-Gaussian model.

The breathing process, as follows from the proposed model, is a two-phase process with a stepwise variable dispersion during the transition from the inhalation phase to the exhalation phase. To study the statistical characteristics of each of the phases of respiration, it is necessary for solving the classification problem of recognizing the phase states of the process, which differ in variances (intensity). It should be noted that for such processes there will be an optimal classification threshold when solving the burst/pause (inhalation/exhalation) recognition problem, minimizing the probability of a complete classification error [3].

4 Frequency Domain Analysis of Respiratory Sound

4.1 Respiratory Rate [4–7]

Respiration rate is the frequency at which respiration occurs. This is usually measured in breaths per minute and is set and controlled by the respiratory center. For humans, the typical breathing rate of a healthy adult at rest is 12–16 breaths per minute. The breathing center sets a quiet breathing rhythm at about two seconds to inhale and three seconds to exhale. This gives the lower of the average frequency of 12 breaths per minute. Average resting respiratory rates by age are:

birth to 6 weeks: 30–40 breaths per minute;
6 months: 25–40 breaths per minute;
3 years: 20–30 breaths per minute;
6 years: 18–25 breaths per minute;
10 years: 17–23 breaths per minute;
Adults: 15–18 breaths per minute;
Elderly $\geq$ 65 years old: 12–28 breaths per minute;
Elderly $\geq$ 80 years old: 10–30 breaths per minute.

The increased respiration rate (tachypnea) develops as a result of the presence of certain pathological conditions [3]. At the same time, it can be expected that the level of noise during inhalation will also be reduced.

4.2 Averaged Spectra and Spectrograms of Respiratory Sound

Since, as already mentioned, the breathing process is significantly non-stationary, and its characteristics during inhalation and exhalation differ significantly, it is necessary to develop a methodology for studying the dynamic variability of the noise spectra during breathing [8]. For this purpose, the average spectra and spectrograms were estimated at different frequency resolutions for lung murmurs during normal vesicular respiration, i.e., studies were carried out for respiratory sound when the lungs are normal—Fig. 4a. The variable parameter was the segment duration, by which the spectrum (FFT) was estimated from 1024 samples (frequency resolution about 43 Hz) to 65,536 (0.67 Hz resolution). A 64-fold change in resolution has practically no effect on the overall shape of the spectrum; however, due to a 64-fold narrowing of the bandwidth (frequency resolution), the spectral density level also decreases by about the same factor. Several areas can be distinguished in the spectra. The frequency of the maximum spectral density lies in the range 170–200 Hz. In the energetic region, spectral densities are up to -40 dB relative to a maximum of about 100–400 Hz.

Besides the average spectra, it is significant and interesting to study the dynamics of changes in spectral characteristics in different phases of respiration, as well as

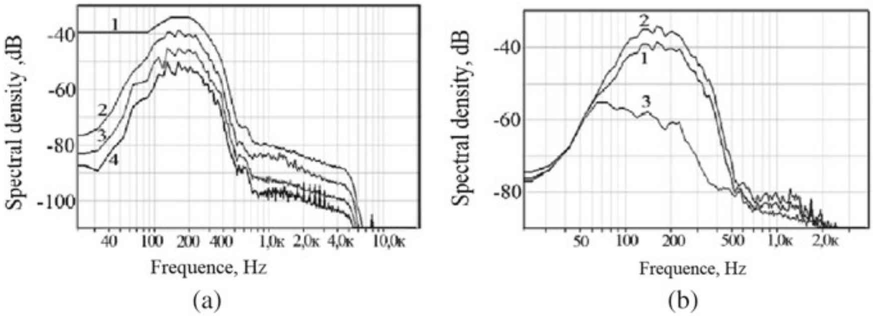


Fig. 4 **a** Spectra of respiratory Sound during vesicular breathing: sampling frequency 44,100 Hz, the number of samples used to build FFT (frequency resolution Hz) 1024 (43.07)—1; 4096 (10.77)—2; 16,384 (2.69)—3; 65,536 (0.67)—4. **b** Spectra of respiratory sound at different breathing phases and a sampling rate of 44,100 Hz. Spectra: 1—Full, 2—Inhalations, 3—Exhalations during vesicular respiration

the interval that must be used when performing the windowed Fourier transform. Figure 4b shows the spectra of the complete and phases of inspiration and expiration during vesicular respiration. Figure 5 shows the spectrograms of normal vesicular respiration at different frequency resolutions. Since the main energy of the sound is concentrated in the inspiratory phase, the full spectrum and spectrum of inspirations differ insignificantly. The spectra of expirations have a significantly lower level in Fig. 4b and Fig. 5a–c. And Fig. 5d shows the spectrograms of vesicular respiration at the initial stage of pneumonia.

It can be seen that for pneumonia, the changes occur in the spectrogram of respiratory sound, which is manifested as a broadening of the spectrum. During normal vesicular respiration there are spectral components in the band up to 500 Hz, and with pneumonia already in the band up to 1000 Hz.

5 Conclusions

The quantitative analysis of respiratory sounds provides a new auxiliary tool for clinical diagnosis. Its frequency domain analysis can make the pathological characteristics of respiratory systems more obvious. The respiratory sounds of patients with lung pneumonia are significantly different, and their high frequency components are significantly higher than the respiratory sounds of normal people. The use of respiratory sounds as a pathological criterion for lung disease has been confirmed.

The future work is to establish a convenient family doctor system to help patients with lung disease self-diagnose and monitor their condition. The effects of heart sounds and ambient respiratory noise need to be further separated to make the results more accurate.

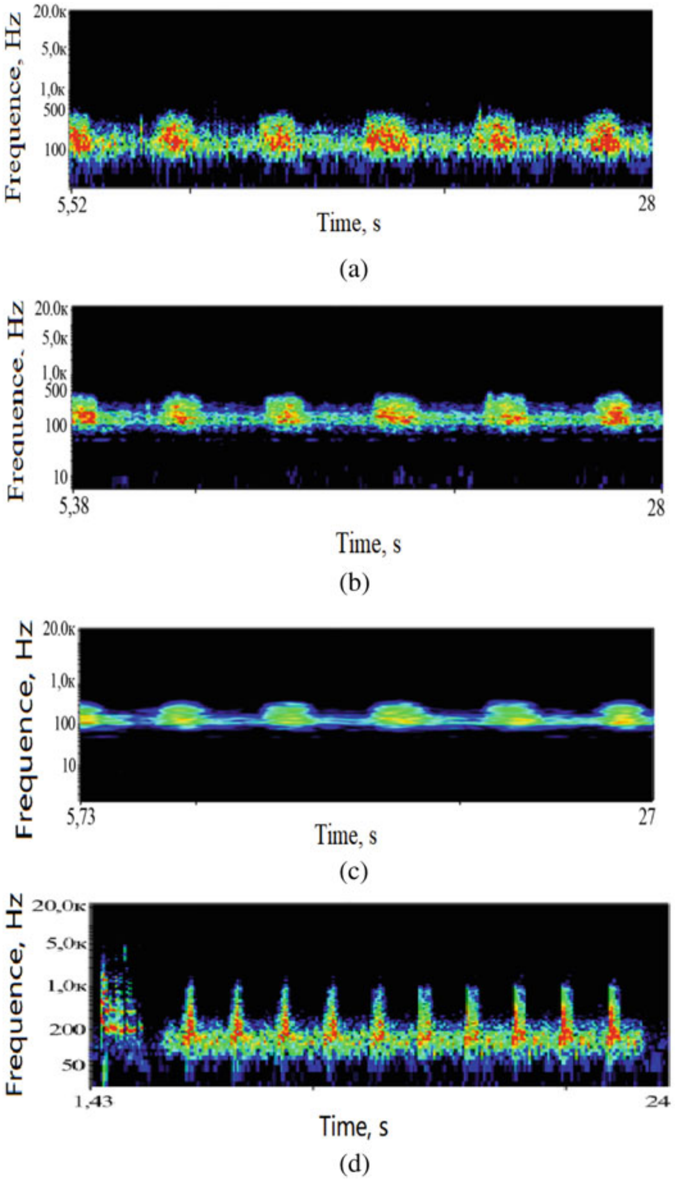


Fig. 5 Spectrograms of normal vesicular respiration at different frequency resolution: **a**—4096 samples (resolution 10.77 Hz), realizations overlap 0%; **b**—16,384 samples (resolution 2.7 Hz), realizations overlap 75%; at—65,536 samples (resolution 0.67 Hz), overlap of realizations 94%; sampling rate 44,100 Hz. Ande spectrograms of vesicular respiration at the initial stage of pneumonia: **d**–**a**—4096 samples (resolution 10.77 Hz)

This work is supported by the National Academy of Sciences of Ukraine and the Ministry of Industry and Trade of Vietnam.

References

1. Lusenko V, Lusenko I, Luo Y, Babakov M, Nguyen A (2020) Signature extraction technologies from acoustic noise of the breathing process in lung pathologies. In: 2020 IEEE Ukrainian microwave week (UkrMW), pp 590–593
2. Dalmay F, Antonini MT, Marquet P, Menier R (1995) Acoustic properties of the normal chest. Eur Respir J 8(10):1761–1769
3. Kravchenko V, Lutsenko V et al (2020) Simulation model of acoustic noises of the respiratory process and technologies of isolation of signatures of lung pathologies. Phys Bases Instrum 3(37):64–67
4. Barrett KE, Barman SM, Boitano S, Brooks H, Ganong's: Rev Med Physiol, 24 edn. p 619
5. DeBoer SL (2004) Emergency newborn care. Trafford Publishing, p 30
6. Lindh WQ, Pooler M, Tamparo C, Dahl BM (2009) Delmar's comprehensive medical assisting: administrative and clinical competencies. Cengage Learn 573
7. Rodríguez-Molinero A, Narvaiza L, Ruiz J, Gálvez-Barrón C (2013) Normal respiratory rate and peripheral blood oxygen saturation in the elderly population. J Am Geriatrics Soc 61(12):2238–40
8. Gavriely N, Palti Y, Alroy G (1981) Spectral characteristics of normal breath sounds. J Appl Physiol Respir Environ Exerc Physiol 50(2):307–314

Emergent Insight of the Cyber Security Management for Saudi Arabian Universities: A Content Analysis

Hamzah Hadi Masmali and Shah J. Miah

Abstract While cyber security has become a prominent concept of emerging information governance, the Kingdom of Saudi Arabia has been dealing with severe threats to individual and organizational IT systems for a long time. These risks have recently permeated into educational institutions, thereby undermining the confidentiality of information as well as the delivery of education. Recent research has identified various causes and possible solutions to the problem. However, most scholars have considered a reductionist approach, in which the ability of computer configurations to prevent unwanted intrusions is evaluated by breaking them down to their constituent parts. This method is inadequate at studying complex adaptive systems. Therefore, the proposed project is designed to utilize a holistic stance to assess the cybersecurity management and policies in Saudi Arabian universities. Qualitative research, entailing a thorough critical review of ten public universities, will be utilized to investigate the subject matter. The subsequent recommendations can be adopted to enhance the security of IT systems, not only in institutional settings but also in any other environment in which such structures are used.

Keywords Cybersecurity · Public universities · Cybercrime · Educational institutes

H. H. Masmali (✉)
School of Electrical Engineering and Computing, The University of Newcastle, Newcastle, NSW, Australia
e-mail: hmasmali@jazanu.edu.sa

College of Business Administration, Jazan University, Jazan, Saudi Arabia

S. J. Miah
Newcastle Business School, University of Newcastle, Callaghan, NSW, Australia
e-mail: shah.miah@newcastle.edu.au

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_14

1 Introduction

Information security is among the top concerns for virtually all organizations across the globe. Firms intending to protect their data have to identify all gaps that may increase their vulnerability, as well as procedures of averting the potential of misusing critical records [1]. More importantly, the mere development and implementation of seemingly adequate data security policies and guidelines to safeguard themselves from potential risks are not enough. Organizations have to continuously create, maintain, and improve their security systems to mitigate both internal and external threats [2]. Nevertheless, the proliferation of portable storage, wireless, and other computing technologies has significantly increased the cybersecurity risks that many companies face.

Many universities in today's world admit that they are struggling to deal with issues related to cybercrime, particularly on access to innovative ways of managing and protecting data [3]. The public-funded universities are particularly financially vulnerable compared to private ones. Consequently, such economically challenged institutions are open to collaborative efforts. Besides, education facilities have limited or no control over the websites since they are accessible to students and teachers who can even login using their devices [4]. Furthermore, schools receive new students every year while others complete their educations, therefore, building a tidal wave of cyber insecurities. To that effect, learning institutions should come up with a holistic move toward striking a balance and ensuring data is protected without prohibiting or blocking students from accessing the platforms. While the region's education system is striving to provide world-class quality for learners' and teachers' experience, they seem to lag in Information Technology (IT) security [5]. It is vital that they adequately invest in defending cybercrime incidences by adopting the right technologies.

The exponential growth, progress, development and complex possibilities that the cyberspace provides for all sectors have been the cause for concern in recent days. Cybercrimes are on the rise and breach of cybersecurity is a threat that needs to be handled ethically, legally, scientifically and quickly since our lives depend on cyberspace [6]. Schools, colleges and universities have started to capitalize on the multiple options provided by cyberspace and are using it extensively for both academic works as well as all kinds of official work. With so much sensitive data being handled, authorities must focus on cybersecurity so that the data remains safe and out of reach of wrong hands. This study looks into the cybersecurity management and policies of 10 selected universities in Saudi Arabia.

The research focuses on the policies and approaches of the universities for maintaining the cybersecurity level. The cybersecurity awareness is important for the universities for protecting the information assets and maintaining the privacy of the management and students. The knowledge and application of the global policies and regulations for cybersecurity can be useful for the university managements to overcome the impact of the hacking, malware attack, phishing of the data and misuse of the cloud storage. In addition to this, information and knowledge of the multilayer cybersecurity approach is the best way to protect the data and systematically manage the information. The research will make emphasis on the combination of firewalls, software and variety of tools that will help the universities to combat the situation of a cyberattack or consulting the experts for managing the digital attack on the university data [7]. There are different types of AI tools that have been used to overcome the malicious cybercrimes. The knowledge and understanding of the cyber policies and approaches will help the universities of Saudi Arabia to improve the level of security.

2 Background of the Study

2.1 Cybersecurity

Cybersecurity is the organization and selection of tools, procedures, and mechanisms used to secure sensitive information in cyberspace from unauthorized and criminals who might damage, misalign or harm organizations [8]. This indicates that only authorized people can have access to sensitive information, such as software, hardware, data, and network in cyberspace. This is a clear definition relating to cybersecurity management in the education sector. There is a serious need to examine the potential cybersecurity risks that organizations face, especially regarding confidential information [9]. Present-day's cyber configurations go beyond the hardware and software components. They also include systemic economic, social, and political aspects that are so interconnected that it has become virtually impossible to isolate the human element from the IT systems [10]. Although existing literature provides a wealth of knowledge on the social facet's influence on cyber operations, it does little to explain its relationship to cybersecurity.

According to [11], cybersecurity is the practice of defending computer, servers, mobile, and electronic devices as well as networks from malicious attack. This type of term is known as information technology security and applied for a variety of context from the business. There are different types of cybersecurity functions are used for managing cybersecurity. This includes network security, application security, information security, and operational security. These processes are having a significant impact on the promotion of cybersecurity and influence the approach of businesses and organizations. However, there are different types of threats that are influencing the approach of the management to maintain the effectiveness in cybersecurity. The education, medical, and public entities are facing the various issues related to cybersecurity that influencing the data management and increasing the threats. The types of threats involve the cybercrime that includes targeting the system for financial gain. The second form of threats is cyberattacks that are politically motivated for the gathering of the information for personal benefits. The third is cyber terrorism that is intended to undermine the electronic system to increase the fear in Internet users.

2.2 ICT Application and Security Issue

The field of information and communication technology (ICT) has evolved with time. It has significantly increased any country's responsibility concerning citizens' security, in addition to having both peaceful and non-peaceful uses [12]. This technology helps provide easy and secure ways of reaching valid information. In contrast, it can also lead to identity theft or access to personal information without permission, i.e., cyberattacks. Cybersecurity is the term used for the security of data. While this field affects multiple disciplines, the most significant sector affected by ICT is education. In the current scenario, the universities are using the ICT tools for managing the educational activities that help to maintain the communication 24*7. The online communication and sharing of the information are allowing the students and professors to get knowledge of process and issues. The implementation of ICT in education is increasing the value to teach and learning by enhancing the effectiveness by utilizing the videos and audio files. People connected to the Internet using different devices such as computers, tablets, and smart phones [6]. The networking system of universities involves the administrative, management, and educational data. The protection of these kinds of data is the major priority of the universities as it can harm the trust and reputation of the organization. The universities are become more concerned about cyber issues and using the different tools and technologies to overcome the threats.

The issues with ICT related to security are involving the privacy means, lack of understanding of the utilization of the tools and applications for connecting with the portal of the university. The third-party vendor services and unauthorized access to the data is also a big security threat for universities that are using the ICT services. In addition to this, the lack of knowledge related to ethical and legal policies for managing the data and security level is influencing the utilization of the technology. As per the views of the Ullah et al. [13], the Distributed Denial of Services (DDoS) attacks are a most common type of cyber issues in ICT that affecting the level of education venue. The motive of such attack is to disruption to the institute's network, system or data center that harms the productivity and system approach of the university. The target of such attack is poorly managed and protected portals of the universities. Another issue related to security for ICT is data theft. This affects the level of education by stealing the data of the students and staff such as name, mobile numbers, address, bank details, and email. The hackers are selling the information to the third-party or used as a bargaining tool and extort money.

The Internet, which is the flagship product of ICT, is a strong tool for cultural exchange and a source of wealth for human civilization. The Internet offers people freedom never previously acquired a possibility of escape, but also of exchanges. While the relationship between different peoples through the network has its advantages, it is also dangerous and complex. The term cybercrime was born at the end of the 90s, with the explosion of exchanges via 'the net'. This period was marked by increasingly frequent infringements on the Internet, such as violations of the rights to privacy or confidentiality. The arrival of the Internet, from the top debit, has led to the emergence of a new criminality category, cybercrime. Therefore, it was necessary to set up legislation to adapt to this new type of crime [14].

In the current scenario, major universities are offering the course through an online platform that is helping in engaging the students and staff members. The online classes and workshops help provide flexible learning and maintain communication among professors and students. The universities have developed websites that offering information related to the course and providing the study material. The students can log in into the portal through personal email id. This kind of facility is having a framework for maintaining the security as personal information of students and university management may not be used for personal benefits. Apart from this, the issues related to cyber hacking and data manipulation harming the reputation of the universities. The challenges related to cybersecurity issues that universities are facing in the current scenario involve the regulatory compliance, third-party vendor services, lack of expertise for protecting the data and open culture [15]. These issues are affecting the approach and work of universities in Saudi Arabia. University management needs to improve the security level to maintain the effectiveness and trust of the staff and students. The management is looking for improvement in cybersecurity by applying the new technology and verification codes that help in protecting the unauthorized access and hacking.

Research Questions

1. What are the major cyber threats for the universities of Saudi Arabia?
2. Are the universities able to handle the threats?
3. What are the policies that could be useful for the universities to overcome the threats of cybersecurity?

This study empirically investigates and appraises the present state of cybersecurity management and policies of ten public universities in Saudi Arabian, with a specific focus on the potential cybersecurity breaches. It is important to have certain supporting objectives to complete the assessment:

- The first objective is identifying the risk and threat caused by cybercriminals against the universities in Saudi Arabia. There is a significant lack of risk and threat when it comes to cybersecurity for higher education regarding the importance and scale of a large volume of sensitive data.
- Second objective by examining whether the universities are ready to handle the threats and risks they face. Preparation must be determined by the level of cybersecurity management in the universities.
- Third objective by suggesting recommended policies to enhance the management of cybersecurity in the universities. The process of selecting and identifying specific recommendations will be driven by providing evidence including a recommendation in the context of research.

The implementation of cybersecurity measures requires large investment for software and firewalls. In addition to this, cultural issues like bring your own devices to increase the challenges for the universities to develop a secure wider network. By providing the basic training to the management and students for using the network and access of the personal portal can help secure the data. The management can provide a simple handbook for policies and tips for practising good cybersecurity hygiene. This kind of training and sharing of the information can be useful for the users to protect the network and all access points that could reduce the issues related to cybercrime with their accounts. Another cost-effective approach to protecting the data is the implementation of multi-factor authorization [16]. This will involve extra security steps for users to login into their account onto the network. This will prevent unauthorized access and help to improve the security level. If the users follow the MFA tool for authentication can be helpful to improve the network security and managing the tasks according to the policies of the university. The end-users security software is providing the facility for scanning the computer for malicious codes and support to remove them from the computers. According to Pandey and Misra [17], the Master Boot Record (MBR) technique is useful for the encryption of the data and hard drives and detecting the threats. The implementation of electronic security encryption is helpful for the real-time detection of the malware issues through analysis of the heuristic and behavioral analysis of the program or code. The proper monitoring of the network and devices can be a good approach for protecting from the cyber issues and improves the security. The knowledge of the potential behavior of the programs and devices is useful for identifying the issues that could lead to cybercrime.

2.3 *Increasing the Complexity of Cybercrime in the Education Sector*

As stated above, universities contain a large amount of data regarding students' personal information. The following research studies are the top cybersecurity factors that businesses or the education sector today must consider [18]

- Increasing complexity, frequency, and scale of cybercrimes
- Leakage of sensitive data, malicious or inadvertent
- Loss of intellectual property
- Strengthening of regulations
- Interconnection of company networks and process control networks

Employees' cybersecurity awareness is an essential factor for preventing and securing organizations from cyber threats and to be aware of security threats while using the Internet [19]. Employee's usage of the Internet has become an integral part of any organization's everyday operations. Technologies also provide opportunities to exploit new markets and respond to the specific needs of clients. University employees' understanding of cybersecurity awareness is essential considering their daily use of the Internet. Since the beginning of the technology revolution, higher education institutions start following technological innovation and digital transformation techniques [18].

Universities face several issues in changing the traditional education system to an eLearning system. Operational risk is one of the challenges faced in this transformation process. There are some policies and tips for protecting from the cyber issues that involve timely update the software and operating system of the device and the network. This will help in implementing the latest security patches for improving the security level. In addition to this, the utilization of the antivirus software will be helpful for the management to identify and remove the potential threats from the computer that could harm the data and files. The trick and knowledge related to not opening the attachments from the unknown senders and links can be useful for protecting the devices from infected malware [20]. Moreover, university management needs to set strong passwords and validation codes for restricting unauthorized access.

2.4 Prevention Measures from Cyberattack

The universities need to craft improvement in the measures and policies to protect the data from the cyberattack. These organizations are facing various issues and challenges that are affecting the reputation and trust of the stakeholders which directly affect the financial gain of the universities. According to Puthal et al. [21], there are different types of approaches available for protecting the data and computer from the cyber-attack or other digital crimes. The foremost approach for protecting the computer from the cyberbullying of attack is providing the knowledge and information related to security principles of the management or other users of the network. This is an economical and simple step for improving cybersecurity. In addition to this, the use of firewalls for the Internet connection can be useful to increase the level of security and overcome the issues related to data theft. This is a major issue for the universities to maintain the secure network connection and check the IP addresses of users to identify the unauthorized access into the portal. Apart from this, it is necessary to secure the Wi-Fi network for improving the safety as it will limit the access of the network and control the unauthorized access into the network. This could be useful for the universities to manage the security operation and identifies the potential threats by optimizing the security checking. The proper monitoring and standers approaches for login and access of the university data can help to craft improvement in the networking and offering the online education and information to the students and staff members.

3 Research Methodology

For conducting the research successfully and in the right manner, the researcher needs to determine the method of the research. The selection of the right method is beneficial for achieving the goals and objectives. To choose the right method for the research, the consideration of three aspects is essential such as divers, barriers, and segmentation. The method of research involves the quantitative and qualitative and mix type. Qualitative method of research is applied for collecting the data that influence the opinion of the people to examine and explaining the facts considering the aim and objectives of the research. This method is allowing the researcher to collect and analyze the secondary data from the authentic sources and critically analyze the different aspects of the topic of the study [22]. The quantitative method of research is applied to discussing the hypothesis derived from the theories. This kind of method is beneficial for the analysis of the objectives of the study. Apart from this, the mixed method of research is used for overcoming the drawbacks of both qualitative and quantitative methods of research and involve theoretical and numerical data to improve the validity and reliability of the research and meet the objectives more professional manner [23].

For the current research, the researcher has applied the qualitative method for collecting the data and analysis. According to this method, the researcher has collected the non-numerical data from the websites of the universities of Saudi Arabia to critically analyze the policies related to cybersecurity. This has helped to gain the information related to management and cybersecurity concern and approach of the universities of Saudi Arabia (See Appendix A for the list of the universities). Apart from this, the researcher has observed the policies of the universities to get knowledge of the measures implemented for protecting the data and piracy of the management.

3.1 Research Approach

To conduct the research, there are two types of research approaches that have been used that involve the inductive and deductive types. The inductive approach of research is used for developing theories considering data analysis and observation. Apart from this, the deductive approach is used for proving the theory by making emphasis on the aim and objectives of the research. This kind of approach is useful for discovering new phenomena considering the findings of the previous studies and analyzing the different perspectives that could help in supporting the arguments of the current research. This is a good technique for identifying the gaps in the research and maintaining the focus on the current standards. However, the indicative research is more open and helping to get the knowledge and understanding of the existing situation but having less concern over the past studies for developing the theory [24].

For the current research, the researcher has applied the deductive approach for analyzing the cybersecurity management and policies of the Saudi Arabian universities. The kind of approach has allowed the researcher to collect the primary data from the websites of the universities and compare the policies for managing cybersecurity. This kind of approach has also helped to develop a valid and reliable conclusion by using the data available through the authentic sources and explaining the concept and variables that have influence the findings of the study. The consideration of existing data and information has helped in proving the theory and satisfying the aim and objectives of the study to meet the desired outcome to analyze the issues that affecting the networking, data interchange and offering the information to management and students using the online portal of study in a secure manner.

3.2 Research Design

Research design is an important element for managing and systematically completing the study. This section of the study is providing the detail information related to the what questions need to be answered and when will be the study carried out as well as what type of data is going to be used for conducting the study. In addition to this, the research design is helping the researcher to select the technique for collecting and analyzing the data according to the type of study. There are three types of designs have been used for managing the study that involves the descriptive, exploratory, and casual. The descriptive design of the study is used for collecting and analyzing the information related to large and specified groups by focusing on the two variables of the study. The exploratory design is used for analyzing the issues by making emphasis on the objectives of the study. This design is flexible and supports the researcher to explore the new ideas and plan the actions that help in meeting the aim of the study. Moreover, it is providing insight into more subjective matters that influence current policies and standards of the chosen topic [25]. Apart from this, the casual design of the research is applied for analyzing the cause effect relationship of the study and determining the flow of the data collection approach using the various techniques.

For managing the current research for analyzing the cybersecurity management and policies of the Saudi Arabian universities, the researcher has selected the exploratory research design. This design helps complete the qualitative research and gain an understanding of the issues and approaches a more professional manner. By using this design, the researcher has done the strategic planning for maintaining the research in a systematic manner that has saved the time for collecting the data from the websites of the universities. The utilization of flexible sources for completing the research has also helped to invalidate the data and increasing the reliability as data is collected from the unbiased sources. Moreover, the researcher has involved the users and included the internal reports of the universities based on cybersecurity and threats to improving the authenticity of the study. This kind of design and approach has helped the researcher to conclude the study simply and more easily by focusing on the aim and objectives of the study.

3.3 Data Collection

Data collection is an important aspect of the study that driver the whole research and influences the overall actions and outcome of the research. To increase the validity and reliability of the research, the researcher needs to collect the authentic data and support the aim and objectives. However, this research collected the data from the websites of the Saudi Arabian universities to understand the policies and measures that applied by the management for overcoming the threats of the data hacking, phishing, and unauthorized access into the portal. Apart from this, the consideration of information provided in the literature review has also helped in supporting the arguments and discussion of the finding. This kind of data collection approach of the researcher has also supported in minimizing the cost of the study and completing it in the estimated time.

3.4 Sampling and Data Analysis

To conduct the primary research, the researcher needs to define the sampling method and size of the sample. The prior identification and selection of the population and characteristics of the respondents are helpful for the researcher to develop a logical conclusion from the finding of the data analysis. For the sampling, there are two types of methods have been used that involve the probability and non-probability sampling. The probability sampling method is applied when the researcher knows the entire population. Apart from this, the non-probability methods are applied where the researcher is free for choosing the sample according to own convenience [26]. Now, to complete the study about analyzing the cybersecurity management and policies of Saudi Arabian universities, the researcher has applied the non-probability method and selected the sample size of 10 universities of Saudi Arabia.

Data analysis is the most important part of the research that helps in developing the valid conclusion and meets the objectives and aim of the study. The current study is based on the qualitative type and exploratory research design. Therefore, the researcher has chosen the thematic and frequency distribution analysis method for the analysis of the data collected through the primary method. The researcher has developed the themes based on the questions and evaluated the collected data. To maintain the systematic approach for the presentation of the data, the researcher has developed the graphs with an interpretation of the respondents related to the challenges and policies of the universities. This kind of presentation will help the readers to understand the response and approach of the analysis that used for evaluation of the data [27]. Moreover, this kind of approach is beneficial for maintaining transparency and offering the recommendations to maintain the effectiveness in the cybersecurity for the universities of Saudi Arabia. Apart from this, the researcher has provided a discussion over the findings of the analysis to satisfy the aim and objectives of the research.

4 Data Analysis

The important part of the research is the data analysis which provide the right information related to the study and help the readers to understand and well knowledge the process of the researcher evaluate the sample to meet the aim and objectives of the research. The researcher has developed different theme by focusing on the approaches of the selected universities and analyzed of their websites and students portals. Furthermore, the researcher has observed the actions and approaches of the students and staff to get the access of the information using the websites of the universities. This can help to understand the related actions and issues of the universities as well as own experience by analyzing through the cyber policies and standards of the universities.

Theme 1: Experience of Cybersecurity at University
There are many universities in Saudi Arabia that offering different types of courses and classes according to global standards and providing support to the students through the website. The management has developed a dynamic website that offers the information related to course, library and future activities in the time of COVID-19. According to the analysis of the 10 universities websites from Saudi Arabia, the leading universities like King Abdulaziz, Jazan University, King Faisal University and Qassim University have updated the privacy policies for the cybersecurity and protection of the data. The managements have developed the sites that have protection for unauthorized access and seeking for the registration before login into account of the university. The knowledge is the legal framework and follow us with the regulations for the cybersecurity guidelines is supporting the universities to maintain the quality network and provide the safety for the users of the website. Apart from this, the King Fahd University of petroleum and minerals, University of Hail and Taibah University are not secured according to the guidelines of the IT to protect the content and information of the visitors of the sites and students. The changes in the current policies and guidelines for the cybersecurity are not updated in the websites if the universities and having a negative impact on the privacy and leading toward the issues like hacking and phishing. Now, the management of the universities need to understand the challenges and get the support from the IT companies to increase the security level and maintain the good practices for storing and access of the accounts of the staff and students.

Theme 2: Major Issues Observed
According to the analysis of the online portal of the universities of Saudi Arabia, it can be considered that some of the online portals are having good practices related to maintaining cybersecurity. The universities such as Jazan University, Qassim University, King Abdulaziz, and King Khalid University have implemented the protocols and applied tools that are checking the IP addresses and approach of the users to maintain the security. The issues that identified in the online education process involve the phishing of the data, data leakage, and IoT ransomware. These are having a direct impact on the devices that are connected with the network of the organization. The

users are facing the challenges related to the stealing of personal information from their accounts and changes in the bio and other data without their permission. As per the analysis of the websites of the universities, the lack of monitoring and regular updating of the security versions the users are facing issues. Most of the issues have been found in King Fahd University of petroleum and minerals, University of Hail and Taibah University. The users have a complaint about these but lack of concern and response from the management is influencing the issues related to cybersecurity. The phishing of information about the passwords, usernames, and payment details for the course is having a negative impact on the process of the data using the online portals of the universities. The users are not trusting the entities and not providing the personal details through contact services of the websites of the universities. The lack of security measures is having a direct impact on the reputation of the educational institutions and raising the questions for the management to maintain the standards. Moreover, the evaluation of websites related to cyber policies have highlighted the issues related to data privacy as there are no policies for cloud-based data storage and access to it. The universities are not following the General Data Protection Regulation that is defined by the IT authorities of the nation. The leakage of information is a major threat for the students and staff members as it can be used for personal benefits or fraud. The threat of stealing personal data is requiring strict actions from the universities to overcome the threats related to cybersecurity. In addition to this, the Distributed Denial of Services (DDoS) attacks are the most common type of cyber issues in ICT that affecting the level of education venue (Fig. 1).

Theme 3: Awareness of the Policies Related to Cybersecurity

According to the evaluation of the websites of Saudi Arabian universities, it has carried out that only 3 out of every 10 students from different universities are having the knowledge of the policies related to cybersecurity. Most of the network users are not aware of the policies and regulations that need to be considered for maintaining the protection of the data and information they are sharing through the network. Apart

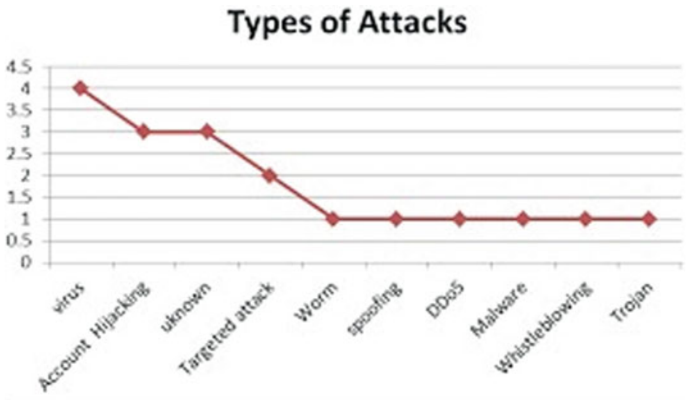


Fig. 1 Cyber issues. *Source* Al-Mhiqani et al. [28, p. 506]

from this, the universities management is not offering any training and information related to the cyber policies that might help in increasing the safety of the data and support in protecting the data. The IT facilities are operated by approval of the university management.

According to the analysis of websites of the universities, there are some policies and privacy-related regulations are mentioned that are helping the users to understand the approach for using the network. The Jazan University, Qassim University, King Abdulaziz, and King Khalid University have implemented the protocols and applied tools and offering the information related to the utilization of the cloud services and use of the protocols for managing the details of the individual. The universities are also offering information for the responsibilities of the individual for using the network and login to the portal. The policies are applied for users and devices of the IT facilities and services and the IT team is configuring the computers and laptops that helping to protect the information and data from hacking and phishing. However, it is the responsibilities of people to get the knowledge and information of the policies and legal obligations to maintain their privacy and protection from the issues related to cybercrime. The management and students have to get the knowledge and understanding of the applicable statutory legislation for maintaining the standards and following the guidelines of the universities. In addition to this, the universities have to provide the information for attack and cyber issues that might cause problems for the individual through advertising and IT support (Fig. 2).

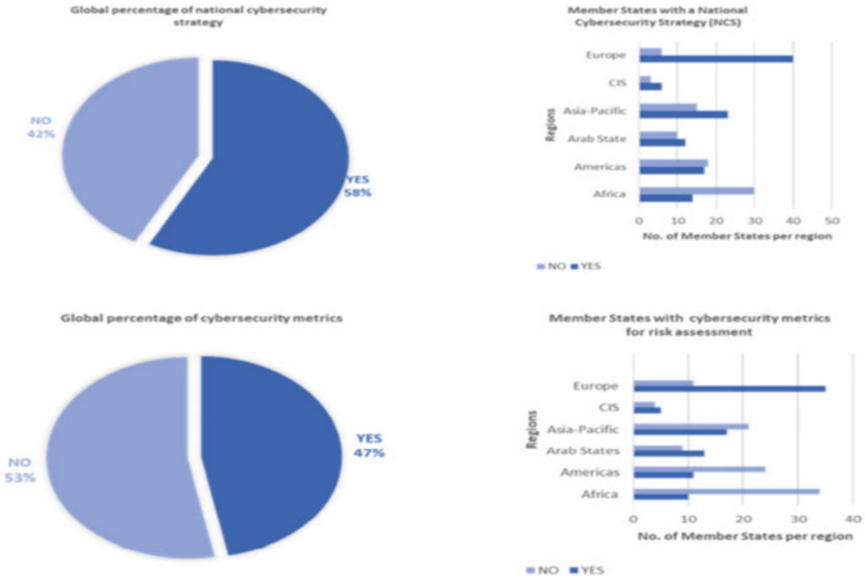


Fig. 2 Global cybersecurity awareness and preparedness per region (29 *Source* Global Cybersecurity Index (GCI) [, p. 18]

Theme 4: Awareness of the Policies Related to Cybersecurity

There are various sources that are offering information and knowledge about the cybersecurity approaches and framework for improving the protection level for the data. To gain the knowledge of cyber policies, the literature review and analysis of website have provided the name of sources such as online articles, discussion with the IT experts, focusing on the privacy policies mentioned on the website of the universities and joining the workshop. All the users of university are not from the technical background and not having much understanding of the issues and cybersecurity. To gain knowledge after facing the issues, the users of the IoT and ICT services of universities are giving preference to reading the online articles and approaches to utilizing the particular software. This kind of approach has helped them to understand the operational process and developing the technical skills that might support in mitigating the vulnerabilities.

The implementation of cyber securities is not having a direct impact on the approach of an individual as hackers are using the advance tools and techniques for phishing and stealing the data. According to the analysis of the policies and framework if university's cybersecurity, it can be considered that major sources of gaining the knowledge of the policies and cybersecurity measures are online reading and follow up of the standards mentioned on the website of the university. The major legislations of the Saudi Arabian government for cybersecurity involve the Telecom Act 2001, Anti-Cyber Crime Law 2009, and Electronic Transaction Law 2007. The management and students of the universities can get information about cybersecurity and approaches by reading these articles and improve practices for controlling, regulating and applying the legal framework for managing the online accounts.

According to the analysis of the websites of universities, it can be considered that Jazan University, Qassim University, King Abdulaziz and King Khalid University, King Fahd University of petroleum and minerals, University of Hail and Taibah University have mentioned the policies and framework for the protection of the data of individual by following the policies. The websites of these universities are offering the knowledge and understanding about the legal information related to security and offering of the personal information to authorized links of the university. The management has clearly stated that the use of privacy control measures as per the government and university approaches for managing cybersecurity is helpful for overcoming the risks (Fig. 3).

Apart from this, the universities are getting the knowledge and understanding from the leading cyber companies for protecting their network, operating system and cloud data. As per the analysis, the major universities of Saudi Arabia are taking assistance from the United States' National Institute of Standards and Technology (NIST) for gaining the knowledge about the cybersecurity functions and improving the policies for the Internet security. In addition to this, the USA organization is offering the knowledge and creating the awareness about the cloud computing that involves the identification of safe and private network for offering the learning and education to the students and providing the facility for the controlling the activities and managing the data safe and secure. Moreover, the organizations have to develop the IT expert desk for offering the information related to the policies and approach for

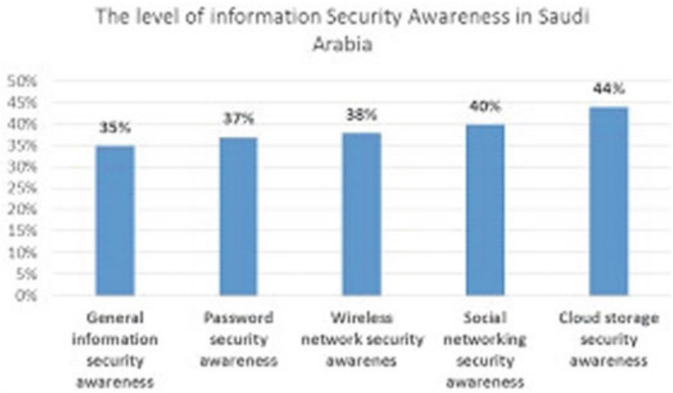


Fig. 3 Knowledge (*Source* Alzahrani and Alomar, p. 134)

the individual to manage the cybersecurity operations. The comprehensive knowledge and information related to security policies will help to overcome the issues. The lacking in monitoring and understanding of the policies are creating threats for Saudi Arabian universities to manage the cyber issues and improve security.

Theme 5: Changes Required for Improving the Cybersecurity

The major changes that suggested by the respondents involve continues development and improvement in cyber defences, monitoring and review of the practices and activities of people who involve in the unauthorized access of the data. Moreover, it is important for the universities to develop the risk audit and compliance committees that are responsible for the implementation of the practices and offering of the information to the management and users. The analysis of sites and cybersecurity policies of universities has suggested that overseeing of the cybersecurity and capability control is also essential for improving the approach of the universities for managing the IT facilities. The framework of universities is lacking and not meeting the standards of operational support facilities. The programmers and testing team is required for supervising and identifying the gaps in the security services and implementation of the support plan to fix it. According to the principles of the data security, the changes that required for mitigating the issues of Saudi Arabian universities involve the adoption, compliance and regulatory management.

There is the requirement of cloud security coordinator center in Saudi Arabia that will look after the equipment and provide the training to the IT experts for creating the awareness about the issues and approaches that help in protecting from cybercrime. As per the analysis, the major requirement for strict implementation and adherence to all current cybersecurity laws in the universities and compulsory training for the management for better understanding of the cloud data and protection.

5 Discussion and Conclusion

The research has analyzed the cybersecurity management and policy issues in Saudi Arabian Universities and identified that there are various issues that are influencing the approach of the staff and students to maintain the privacy and other security measures for data. According to analysis, the university is lacking in infrastructure development and continues improvement in the cyber policies and regulations. The students and management are also not aware of the policies and protection standards that required for improving the data security to maintain the safety of their personal information and digital learning approaches. The research has also identified the computing technologies used by the universities for offering education and securing there data and activities over the network. In addition to this, the study has analyzed that the universities have developed websites that offering information related to the course and providing the study material. The students can login into the portal through personal email id.

In the current scenario, the higher educational institutions are using the digital technologies and devices for offering the learning and sharing of the study material with the students. This is helping to connect with the students and monitor their learning more effective manner. Moreover, this type of learning is also helping the students to get real-time support from the website of the universities by accessing the library by creating the account. However, the cybersecurity issues related to phishing, hacking attack of the various viruses and hacking is influencing the approaches of the individual. There is no awareness about the issues and policies for maintaining the standards of the security which influencing the management approaches and implementation of good practices [3]. The knowledge and application of the global policies and regulations for cybersecurity can be useful for the university managements to overcome the impact of the hacking, malware attack, phishing of the data and misuse of the cloud storage. The issues with ICT related to security are involving the privacy means, lack of understanding of the utilization of the tools and applications for connecting with the portal of the university. Moreover, information and knowledge of the multilayer cybersecurity approach is the best way to protect the data and systematically manage the information.

According to the analysis of the study, the universities of Saudi Arabia are looking to update the cybersecurity measures and policies to increase the standards of cyber activities and actions.

As per the analysis, the implementation of the new technique is involving end-to-end protection. The implementation of electronic security encryption is helping for the real-time detection of the malware issues through analysis of the heuristic and behavioral analysis of the program or code. Apart from this, the study has identified that universities of Saudi Arabia are using different software and suits that are helping to increase the level of cybersecurity. In addition to this, the implementation of cloud-based security protection is helping the universities and management to secure the browsing and protecting from the virus attack as it blocked the site of links.

In addition to this, the lack of implementation of intrusion policies for detecting unauthorized access is also affecting the cybersecurity of the universities. The study has discussed and provided the information related to the implementation of exceptions policy and host integration that can be useful for the universities to protect the data and maintaining the security level. The exceptions policy provides the ability to exclude applications and processes from the detection of the virus and scan the data. In addition to this, host integration is helping the users and network providers to enforce and restore the security of the client computer that influence the level of the security and give the information about the implementation of protocols of accessing the portal. Apart from this, the research has identified the approaches that required the changes in the policies and framework for managing data security at the university level.

By considering the analysis and identification of cybersecurity issues and management approaches of the Saudi Arabian universities, it can be considered that the identified 10 universities are facing different issues. The management has to look into the challenges and have to plan the development for the betterment of the secure network. Following are the recommendations that could be useful for the universities to manage the issues and craft improvement in the cyber policies and implement them strictly:

- The universities can take support from the international agencies that are identifying the issues and developing the tools for protecting the data. The American companies are best in this business and offering the best software and framework that could help the universities to improve the standards. The universities can contact with the NIST of USA for constancy and offering the support for continuous improvement in the policies and infrastructure of the organizations.
- For protecting from the cyber issues and craft improvement in the services options and data management, it is recommended to the university management to conduct the regular monitoring of the servers, devices, network, and approaches of the users. The proper auditing will be helpful for the management to understand the factors that are creating barriers and make real-time efforts to improve the services standards.
- The management of universities has to develop the IT desk for protecting cyber issues. This kind of approach will help in influencing the security measures. The development of the IT expert desk for offering the information related to the policies and approach for the individual to manage the cybersecurity operations. The comprehensive knowledge and information related to security policies will help to overcome the issues. In addition to this, the use of AI tools and technology will be helpful for improving the protection which will monitor the approach of the users and functioning of the operating system.

Appendix A: List of Universities

1. King Abdulaziz University https://www.kau.edu.sa/Home.aspx
2. King fahd university of petroleum and minerals http://www.kfupm.edu.sa/ar/Default.aspx
3. King Faisal University https://www.kfu.edu.sa/sites/Home/
4. King Khalid University https://www.kku.edu.sa/
5. King Saud University https://www.ksu.edu.sa/en/
6. Qassim University https://www.qu.edu.sa/
7. TaibahUniversity https://www.taibahu.edu.sa/Pages/AR/Home.aspx
8. Taif University https://www.tu.edu.sa/
9. University of Hail http://www.uoh.edu.sa/Pages/default.aspx
10. Jazan University https://www.jazanu.edu.sa/

References

1. Dehlawi Z, Abokhodair N (2013) Saudi Arabia's response to cyber conflict: a case study of the Shamoon malware incident. In: Paper presented at the 2013 IEEE international conference on intelligence and security informatics. employee's behavior. Paper presented at the international conference on research and practical issues of enterprise information systems
2. Reid R, Van Niekerk J (2014) From information security to cyber security cultures. In: Paper presented at the 2014 information security for South Africa
3. Cheung RS, Cohen JP, Lo HZ, Elia F (2011) Challenge based learning in cybersecurity education. Paper presented at the proceedings of the international conference on security and management (SAM)
4. Ramim M, Levy Y (2006) Securing e-learning systems: a case of insider cyber attacks and novice IT management in a small university. J Cases Inf Technol 8(4):24–34
5. Rezgui Y, Marks A (2008) Information security awareness in higher education: an exploratory study. Comput Secur 27(7–8):241–253
6. De Bruijn H, Janssen M (2017) Building cybersecurity awareness: the need for evidence-based framing strategies. Gov Inf Q 34(1):1–7
7. Pandey RK, Misra M, (2016) Cyber security threats—Smart grid infrastructure
8. Craigen D, Diakun-Thibault N, Purse R (2014) Defining cybersecurity. Technol Innov Manage Rev 4(10)
9. Slusky L, Partow-Navid P (2012) Students information security practices and awareness. J Inf Privacy Secur 8(4):3–26
10. Benson V, McAlaney J, Frumkin LA (2019) Emerging threats for the human element and countermeasures in current cyber security landscape. In: Cyber law, privacy, and security
11. Alzahrani A, Alomar K (2016) Information security issues and threats in Saudi Arabia: a research survey. Int J Comput Sci Issues (IJCSI) 13(6):129
12. Yeniyurt S, Wu F, Kim D, Cavusgil ST (2019) Information technology resources, innovativeness, and supply chain capabilities as drivers of business performance: a retrospective and future research directions. Ind Mark Manage 79:46–52
13. Ullah F, Naeem H, Jabbar S, Khalid S, Latif MA, Al-Turjman F, Mostarda L (2019) Cyber security threats detection in internet of things using deep learning approach. IEEE Access 7:124379–124389

14. Marcum CD, Higgins GE (2019). Cybercrime. In: Handbook on crime and deviance. Springer, pp 459–475
15. Tweneboah-Koduah S, Skouby KE, Tadayoni R (2017) Cyber security threats to IoT applications and service domains. Wirel Pers Commun 95(1):169–185
16. Lamba A, Singh S, Balvinder S, Dutta N, Rela S, (2017) Analyzing and fixing cyber security threats for supply chain management. Int J Technol Res Eng 4(5)
17. Pandey RK, Misra M (2016). Cyber security threats—Smart grid infrastructure. In: 2016 National power systems conference (NPSC). IEEE, pp 1–6
18. Syed AM, Ahmad S, Alaraifi A, Rafi W (2020) Identification of operational risks impeding the implementation of eLearning in higher education system. Educ Inf Technol 1–17
19. Li L, Xu L, He W, Chen Y, Chen H (2016). Cyber security awareness and its impact on employee's behavior. In: International conference on research and practical issues of enterprise information systems. Springer, Cham, pp 103–111
20. Walker-Roberts S, Hammoudeh M, Aldabbas O, Aydin M, Dehghantanha A (2020) Threats on the horizon: understanding security threats in the era of cyber-physical systems. J Supercomput 76(4):2643–2664
21. Puthal D, Mohanty SP, Nanda P, Choppali U (2017) Building security perimeters to protect network systems against cyber threats [future directions]. IEEE Consumer Electron Mag 6(4):24–27
22. Mohajan HK (2018) Qualitative research methodology in social sciences and related subjects. J Econ Dev Environ People 7(1):23–48
23. Basias N, Pollalis Y (2018) Quantitative and qualitative research in business & technology: Justifying a suitable research methodology. Rev Integr Bus Econ Res 7:91–105
24. Snyder H (2019) Literature review as a research methodology: an overview and guidelines. J Bus Res 104:333–339
25. Wiek A, Lang DJ (2016) Transformational sustainability research methodology
26. Humphries B (2017) Re-thinking social research: anti-discriminatory approaches in research methodology. Taylor & Francis
27. Ulmer JB (2017) Posthumanism as research methodology: inquiry in the anthropocene. Int J Qual Stud Educ 30(9):832–848
28. Al-Mhiqani MN, Ahmad R, Yassin W, Hassan A, Abidin ZZ, Ali NS, Abdulkareem KH (2018) Cyber-security incidents: a review cases in cyber-physical systems. Int J Adv Comput Sci Appl 1:499–508
29. Global Cybersecurity Index (GCI)—ITU: Committed to ... (n.d.). Retrieved 23 Jan 2018 from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Central Bank Digital Currencies (CBDCs) as a New Tool of E-Government: Socio-economic Impacts

Galia Kondova and Patrik Rüegg

Abstract A central bank digital currency (CBDC) in comparison with other forms of digital money presents a direct claim on the issuing central bank. There are three architecture types of CBDC, namely indirect CBDCs, hybrid CBDCs, and direct (retail) CBDCs, all based on blockchain technology. This paper briefly discusses these three types and outlines the major socio-economic effects this new e-government tool could have on the economy.

Keywords CBDC · Digital currency · E-government · Blockchain · Economic policy

1 Introduction

Cryptocurrencies have been on the rise since the launch of bitcoin shortly after the global financial crisis in 2008. The blockchain being the underlying technology behind cryptocurrencies facilitates peer-to-peer transactions in a secure manner without the necessity of a trusted third party and thus promises efficiency gains. Several central banks have been exploring possibilities for the introduction of a central bank digital currency (CBDC), which is digital legal tender based on the blockchain technology [1].

It is worth noting that electronic money is available for quite some time including e-banking transactions, credit card transactions, online transactions, etc. One major difference, however, between digital currency and the CBDC is the way the settlement of transactions takes place. Currently, the processing and settlement of customer transactions are restricted to financial institutions [2]. Thus, the customer faces the risk of default of the financial institution as an intermediary in the transaction. In the case of a direct CBDC, however, the CBDC presents a direct claim on the issuing

G. Kondova (✉)
School of Business FHNW, Peter Merian Str. 86, 4002 Basel, Switzerland
e-mail: galia.kondova@fhnw.ch

P. Rüegg
School of Business FHNW, Riggenbachstr. 16, 4600 Olten, Switzerland

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_15

central bank and the central bank handles all retail payments. This last aspect implies important socio-economic impacts that will be discussed later.

2 CBDC Architectures

According to Auer and Boehme [3], there are three fundamental retail CBDC architectures under discussion, namely the direct, the hybrid, and the indirect CBDC. An overview of the three CBDC types is presented in Fig. 1.

The direct CBDC entitles the holder to a direct claim on the issuing central bank which is also responsible for handling all retail payments. The financial intermediaries or the central bank itself are responsible for the onboarding of the users.

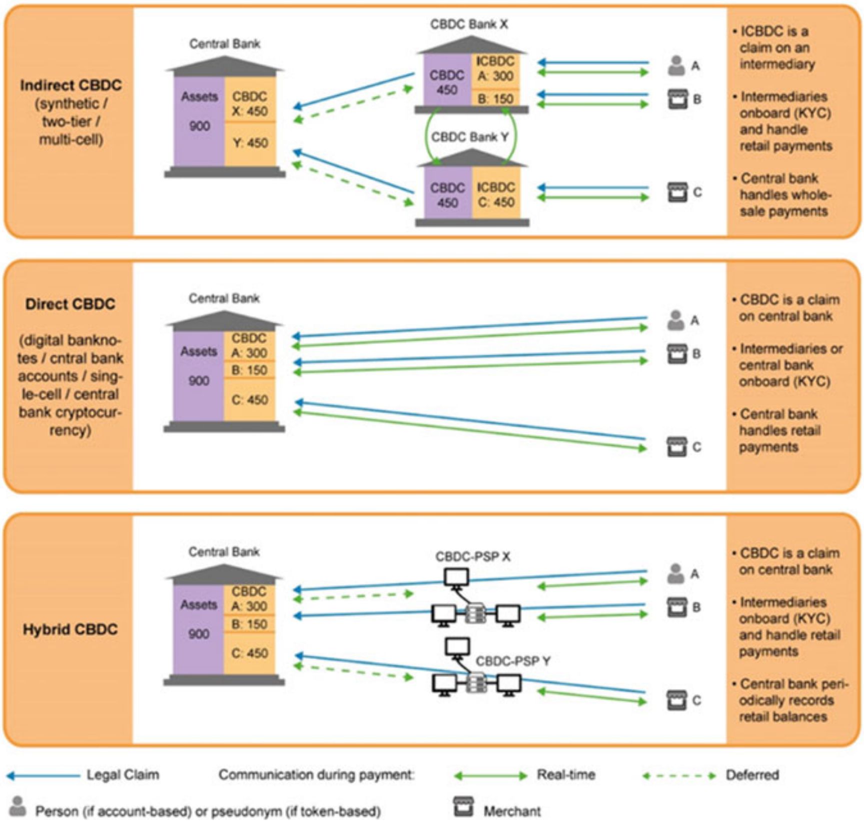

Indirect CBDC
(synthetic / two-tier / multi-cell)
Central Bank
Assets 900
CBDC X: 450
Y: 450
CBDC Bank X
CBDC 450
ICBDC A: 300
B: 150
CBDC Bank Y
CBDC 450
ICBDC C: 450
A
B
C
• ICBDC is a claim on an intermediary
• Intermediaries onboard (KYC) and handle retail payments
• Central bank handles whole-sale payments
Direct CBDC
(digital bankno-tes / cntral bank accounts / sing-le-cell / central bank cryptocur-rency)
Central Bank
Assets 900
CBDC A: 300
B: 150
C: 450
A
B
C
• CBDC is a claim on central bank
• Intermediaries or central bank onboard (KYC)
• Central bank handles retail payments
Hybrid CBDC
Central Bank
Assets 900
CBDC A: 300
B: 150
C: 450
CBDC-PSP X
CBDC-PSP Y
A
B
C
• CBDC is a claim on central bank
• Intermediaries onboard (KYC) and handle retail payments
• Central bank peri-odically records retail balances
Legal Claim
Communication during payment:
Real-time
Deferred
Person (if account-based) or pseudonym (if token-based)
Merchant

Fig. 1 Synthetic, direct, and hybrid CBDC scheme of legal claims and settlement occurrence [3]

The indirect CBDC presents a claim on an intermediary that is fully backed at the central bank. The central bank only handles wholesale payments in this case. The intermediaries are responsible for the onboarding of customers and the settlement of retail payments. The indirect CBDC architecture thus resembles the current two-tier banking system only that it is operated on a new technology, namely the blockchain.

The hybrid CBDC (h-CBDC) incorporates a two-tier structure with direct claims on the central bank while real-time payments are handled by intermediaries. The intermediaries are also responsible for onboarding and handling retail payments.

3 Socio-economic Impacts

To assess the impact of the introduction of a CBDC, it is important to identify the most important stakeholders. These include the central bank, private banks, firms, and consumers [4] for which the following socio-economic impact analysis has been conducted.

3.1 Impact on Consumers

Auer and Boehme [3] highlight the importance of a CBDC providing a "cash-like with peer-to-peer functionality" and offering "convenient real-time payments" in the design of its architecture. Furthermore, the choice of an underlying technology (blockchain or a conventional infrastructure) should be made to ensure "resilient and robust operations." Moreover, decisions on how to deal with consumer information should be made to make sure that the CBDCs are "accessible to all" and "ensure privacy in lawful exchange" [3]. Finally, CBDCs should facilitate cross-border payments.

Bank of England [5] formulates the core CBDC design principles in regards of retail payments as being reliable and resilient, fast and efficient, and innovative and open to competition.

An important consideration is also whether a CBDC is interest-bearing or not, the latter being classified as "cash-like" since bank notes and coins today are not interest-bearing [6].

3.2 Impact on Central Banks

Digital currencies like CBDCs could be considered as a new tool for conducting monetary policy by central banks. Some authors argue that CBDCs could "accommodate features that can potentially amount to granting additional powers to central banks, such as having higher surveillance power over transactions and imposing negative interest rates, which would otherwise be absent or limited" [7].

Bank of England [5] identifies several opportunities from a central bank perspective, namely supporting a resilient payment landscape, avoiding the risks of new forms of private money creation, supporting competition, efficiency, and innovation in payments, meeting future payment needs in a digital economy, improving the availability and usability of central bank money, addressing the consequences of a decline in cash use, CBDC could function as a building block for better cross-border payments. An additional strong advantage could be the availability of a programmable feature to CBDCs based on the application of smart contracts. This would allow for automated money flows or automated interest payments [8].

At the same time, [5] also identifies risks associated with the introduction of a CBDC, namely disintermediation risk (switching from deposits to CBDC, posing a threat to private banks, and therefore the availability of credit to companies and households), financial instability through a rapid flow from deposits toward CBDC (e.g., digital bank run).

3.3 Impact on Banks

The possible introduction of a CBDC has the potential to disrupt the traditional retail banking sector business models by enabling a peer-to-peer financial system without the need of financial intermediaries. Thus, CBDC poses the risk of a loss of the systemic advantage of the banking sector while at the same time increases pressure on banks to keep up with innovations of the FinTech companies.

Banks are already facing strong competition from FinTech companies like the P2P lending platforms in Europe. They effectively provide for provision of credit without bank intermediation [9]. This P2P lending could become even more important with the introduction of a direct CBDC since this would enable a P2P lending in CBDC equal to physical cash borrowing from a friend.

Vives [9] envisages that all these disruptive trends would lead in the long run to the development of a platform economy enabled by a CBDC to offer wide-range, consumer centric financial services in a partnership business model involving all stakeholders.

4 Conclusion

This paper provided an overview of the CBDC architectures under discussion and the related socio-economic impacts.

There are several opportunities related to CBDCs that have been identified in association with payment transactions such as an improved efficiency of cash circulation as well as lower costs of payment transaction. In addition, it is expected that the introduction of CBDCs would facilitate the financial inclusion of private digital payment providers as well as enhance the traceability and monitoring of payment transaction. In terms of monetary policy, the expected benefits are related to a better monetary control due to the real-time data collection.

On the other hand, several socio-economic challenges have been identified in relation to CBDCs such as increased expenses for addressing cybersecurity issues, preventing money laundering abuses, and ensuring system resilience. Moreover, the introduction of a CBDC poses a most significant challenge, namely the one of transforming the existing legacy payment infrastructure without threatening the financial system as a whole.

References

1. Auer R, Cornelli G, Frost J (2020) Rise of the central bank digital currencies: drivers, approaches and technologies. BIS Working Paper No.880
2. Barrdear J, Kumhof M (2016) The macroeconomics of Central Bank issued digital currencies. SSRN Electron J. https://doi.org/10.2139/ssrn.2811208
3. Auer R, Boehme R (2020) The technology of retail central bank digital currency. BIS Quaterly Review. https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf
4. Andolfatto D (2018) Assessing the Impact of Central Bank Digital Currency on Private Banks. Working Paper 2018–026. Federal Reserve Bank of St. Louis. https://doi.org/10.20955/wp.2018.026
5. Bank of England (2020) Central Bank Digital Currency: Opportunities, challenges and design. Discussion Paper. https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper
6. Bank for International Settlement (2020) Central bank digital currencies: foundational principles and core features. Report No. 1. https://www.bis.org/publ/othp33.pdf
7. Nabilou H (2019) Central Bank digital currencies: preliminary legal observations. J Bank Regul. https://doi.org/10.2139/ssrn.3329993
8. Sandner P, Groß J, Schulden P, Grale L (2020) Digitaler, programmierbarer Euro, Libra und CBDCs: Auswirkungen digitaler Zahlungsinitiativen auf europäische Banken. Ifo Schnelldienst. https://www.ifo.de/DocDL/sd-2020-10-sandner-gross-schulden-grale-libra-cbdc.pdf
9. Vives X (2019) Digital disruption in banking. Annu Rev Financ Econ 11:243–272. https://doi.org/10.1146/annurev-financial-100719-120854

An Adaptive Self-modeling Network Model for Multilevel Organizational Learning

Gülay Canbaloğlu, Jan Treur, and Peter Roelofsma

Abstract Multilevel organizational learning concerns an interplay of different types of learning at individual, team, and organizational levels. These processes use complex dynamic and adaptive mechanisms. A second-order adaptive network model for this is introduced here and illustrated.

Keywords Multilevel organizational learning · Adaptive network model · Self-model

1 Introduction

Multilevel organizational learning is a complex, dynamic, adaptive, cyclical, and non-linear type of learning involving multiple levels and both dependent on individuals and independent of individuals. It is multilevel because the learning of an organization involves learning at the level of individuals, at the level of teams (or groups or projects), and at the level of the organization via feed forward and feedback pathways:

> Through feed forward processes, new ideas and actions flow from the individual to the group to the organization levels. At the same time, what has already been learned feeds back from the organization to group and individual levels, affecting how people act and think. (Wiewiora et al. [5], p. 532)

G. Canbaloğlu (✉) · J. Treur · P. Roelofsma
Delft University of Technology, Center for Safety in Healthcare, Delft, The Netherlands
e-mail: gcanbaloglu17@ku.edu.tr

J. Treur
e-mail: j.treur@vu.nl

P. Roelofsma
e-mail: P.H.M.P.Roelofsma@tudelft.nl

G. Canbaloğlu
Department of Computer Engineering, Koç University, Istanbul, Turkey

J. Treur
Vrije Universiteit Amsterdam, Amsterdam, The Netherlands

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_16

> There is growing consensus in the literature that the theory of organizational learning should consider individual, team, and organizational levels. (Wiewiora et al. [15], p. 94)

There is a huge amount of literature on multilevel organizational learning such as [1, 3, 5, 7–9, 14, 15]. However, systematic approaches to obtain (adaptive) computational models for it cannot be found. In the current paper, a self-modeling network modeling perspective is used to model the different adaptive, interacting processes of multilevel organizational learning.

Computational modeling of multilevel organizational learning provides a more observable formalization of multilevel organizational learning and provides possibilities to perform "in silico" (simulation) experiments with it. To this end, the self-modeling network modeling approach introduced in Treur [10] that is explained in detail in Sect. 3 is used in this current paper.

First, Sect. 2 presents how literature provides ideas on mental models at individual, team, and organization level and their role in multilevel organizational learning. Then, Sect. 3 explains the characteristics and details of adaptive self-modeling network models, and how they can be used to model the different processes concerning dynamics, adaptation, and control of mental models. In Sect. 4, the controlled adaptive network model for multilevel organizational learning is introduced. Then, in Sect. 5, an example simulation scenario is explained in detail. Section 6 is a discussion section.

2 Background Literature

The quotes in the introduction section illustrate the perspective adopted here. Mental models are considered a vehicle to model the interplay of learning at individual, team, and organizational level. Individual mental models learnt are a basis for formation of shared team mental models; these shared team mental models provide input for the shared mental models at the organization level. Conversely, these shared mental models at organization and team level are used to improve shared team mental models and individual mental models, respectively. The picture of the different pathways shown in Fig. 1 is a slightly rearranged version of Fig. 1 in Crossan et al. [5] and also strongly resembles Fig. 4 of Wiewiora et al. [15] and Fig. 3 of Wiewiora et al. [14].

Inspired by this, as a basis for the analysis made here, the considered overall multilevel organizational learning process consistsof the following main processes and interactions; see also [5] and Wiewiora et al. [15]:

(a) **Individual level**

(1) Creating and maintaining individual mental models
(2) Choosing for a specific context a suitable individual mental model as focus
(3) Applying a chosen individual mental model for internal simulation
(4) Improving individual mental models

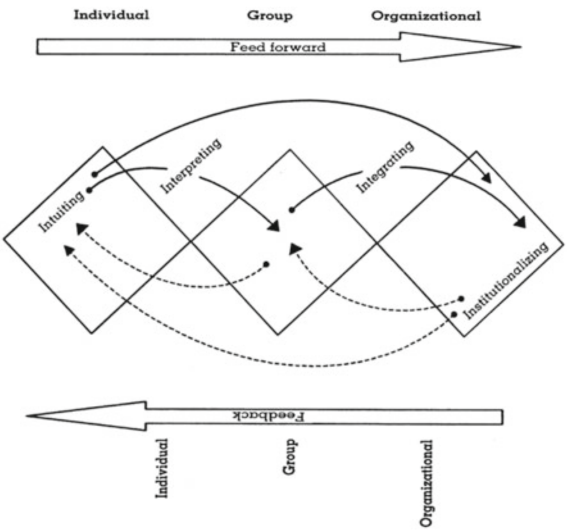


Fig. 1 Dynamics of organizational learning; adapted from Crossan et al. [5], Fig. 1. For a similar picture, see Wiewiora et al. [15], Fig. 4 and Fig. 3 of Wiewiora et al. [14]

(b) **From individual level to team level (feed forward learning)**

(1) Deciding about creation of shared team mental models
(2) Creating shared team mental models based on developed individual mental models

(c) **From team level to organization level (feed forward learning)**

(1) Deciding about creation of shared mental models
(2) Creating shared mental models based on developed individual mental models

(d) **From organization level to team level (feedback learning)**

(1) Deciding about teams to adopt shared organization mental models
(2) Teams adopting shared mental models

(e) **From team level to individual level (feedback learning)**

(1) Deciding about individuals to adopt shared team mental models
(2) Individuals adopting shared team mental models by learning them

(f) **Individual level**

(1) Creating and maintaining individual mental models
(2) Choosing for a specific context a suitable individual mental model as focus
(3) Applying a chosen individual mental model for internal simulation
(4) Improving individual mental models

This overview provided useful input to the design of the computational network model for multilevel organizational learning that will be introduced in Sect. 4.

3 The Self-modeling Network Modeling Approach

In this section, the self-modeling modeling approach [11] used is explained. A network model is defined by (where X and Y are nodes or states of the network):

- *Connectivity characteristics*
  Connections from one state X to a state Y with their weights $\boldsymbol{\omega}_{X,Y}$
- *Aggregation characteristics*

For any state Y, a combination function $\boldsymbol{cc_Y(..)}$ is used to specify the aggregation that is applied to the impacts $\boldsymbol{\omega}_{X,Y}X(t)$ on Y from the incoming connections from states X to Y

- *Timing characteristics*

For each state Y, a speed factor $\boldsymbol{\eta}_Y$ defines how fast it changes for given causal impact.

The following difference equations are used for simulation; they are based on the network characteristics $\boldsymbol{\omega}_{X,Y}$, $\mathbf{c}_Y(..)$, $\boldsymbol{\eta}_Y$ in a canonical manner:

$$Y(t + \Delta t) = Y(t) + \boldsymbol{\eta}_Y[\mathbf{c}_Y(\boldsymbol{\omega}_{X_1,Y}X_1(t), \ldots, \boldsymbol{\omega}_{X_k,Y}X_k(t)) - Y(t)]\Delta t \qquad (1)$$

for each state Y, where X_1 to X_k are the states from which Y receives incoming connections. The dedicated software environment [11, Chap. 9] includes a library with currently around 50 basic combination functions. The examples of basic combination functions that are applied in the model introduced here can be found in Table 1.

By a *self-modeling network* (also called a *reified* network), a network-oriented conceptualization can also be applied to *adaptive* networks; see Treur [10]. Here, new states are added to the network (called *self-model states*) representing network characteristics. These self-model states are depicted at a next level (called *self-model level* or *reification level*); the original network is at the *base level.*

This is often applied to the weight $\boldsymbol{\omega}_{X,Y}$ of a connection from state X to state Y; this is represented by a self-model state $\mathrm{W}_{X,Y}$. Similarly, any other network characteristic from $\boldsymbol{\omega}_{X,Y}$, $\mathbf{c}_Y(..)$, $\boldsymbol{\eta}_Y$ can be self-modeled by including self-model states. For example, a speed factor $\boldsymbol{\eta}_Y$ can be represented by a self-model state H_Y.

This self-modeling network construction can be applied iteratively to obtain multiple orders of self-models at multiple (first-order, second-order, …) self-model levels. For example, a second-order self-model may include a second-order self-model state $\mathrm{H}_{\mathrm{W}_{X,Y}}$ representing the speed factor $\eta_{\mathrm{W}_{X,Y}}$ for the (learning) dynamics of

Table 1 The combination functions applied in the introduced network model

	Notation	Formula	Parameters
Advanced logistic sum	$\mathbf{alogistic}_{\sigma,\tau}(V_1, \ldots, V_k)$	$[\frac{1}{1+e^{-\sigma(V_1+\cdots+V_k-\tau)}} - \frac{1}{1+e^{\sigma\tau)}}](1+e^{-\sigma\tau})$	Steepness $\sigma > 0$ Excitability threshold τ
Steponce	$\mathbf{steponce}_{\alpha,\beta}(..)$	1 if time t is between α and β, else 0	Start time α End time β
Hebbian learning	$\mathbf{hebb}_{\mu}(V_1, V_2, V_3)$	$V_1 * V_2(1 - V_3) + \mu V_3$	V_1,V_2 activation levels of states X and Y; V_3 activation level of the self-model state $\mathbf{W}_{X,Y}$ Persistence factor μ
Maximum composed with Hebbian learning	$\mathbf{max\text{-}hebb}_{\mu}(V_1, \ldots, V_k)$	$\max(\mathbf{hebb}_{\mu}(V_1, V_2, V_3), V_4, \ldots, V_k)$	
Scaled maximum	$\mathbf{smax}_{\lambda}(V_1, \ldots, V_k)$	$\max(V_1, \ldots, V_k)/\lambda$	Scaling factor λ

first-order self-model state $\mathrm{W}_{X,Y}$ which in turn represents the adaptation of connection weight $\boldsymbol{\omega}_{X,Y}$. Similarly, a persistence factor $\mu_{\mathrm{W}_{X,Y}}$ of such a first-order self-model state $\mathrm{W}_{X,Y}$ used for adaptation (e.g., based on Hebbian learning) can be represented by a second-order self-model state $\mathrm{M}_{\mathrm{W}_{X,Y}}$.

In the current paper, the self-modeling network perspective is applied to design a second-order adaptive mental network architecture addressing the mental and social processes underlying organizational learning by proper handling of individual mental models and shared mental models. In this self-modeling network architecture, the base level addresses the use of a mental model by internal simulation, the first-order self-model the adaptation of the mental model, and the second-order self-model level models the control over this; see Fig. 2. In this way, the three-level cognitive architecture described in Treur and Van Ments [11], Van Ments et al. [13]

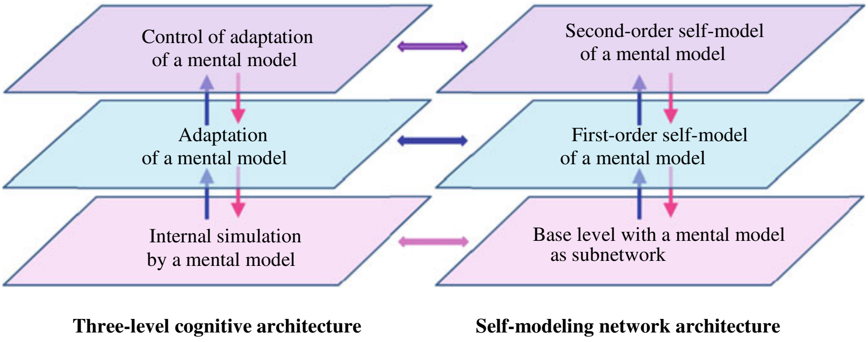

Control of adaptation of a mental model
Adaptation of a mental model
Internal simulation by a mental model
Second-order self-model of a mental model
First-order self-model of a mental model
Base level with a mental model as subnetwork
Three-level cognitive architecture
Self-modeling network architecture

Fig. 2 Computational formalization of the three-level cognitive architecture for mental model handling from Van Ments et al. [12] by a self-modeling network architecture

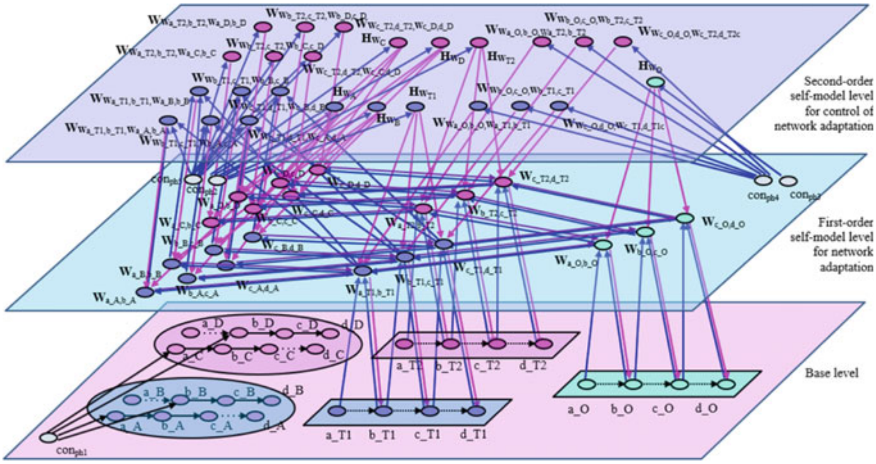


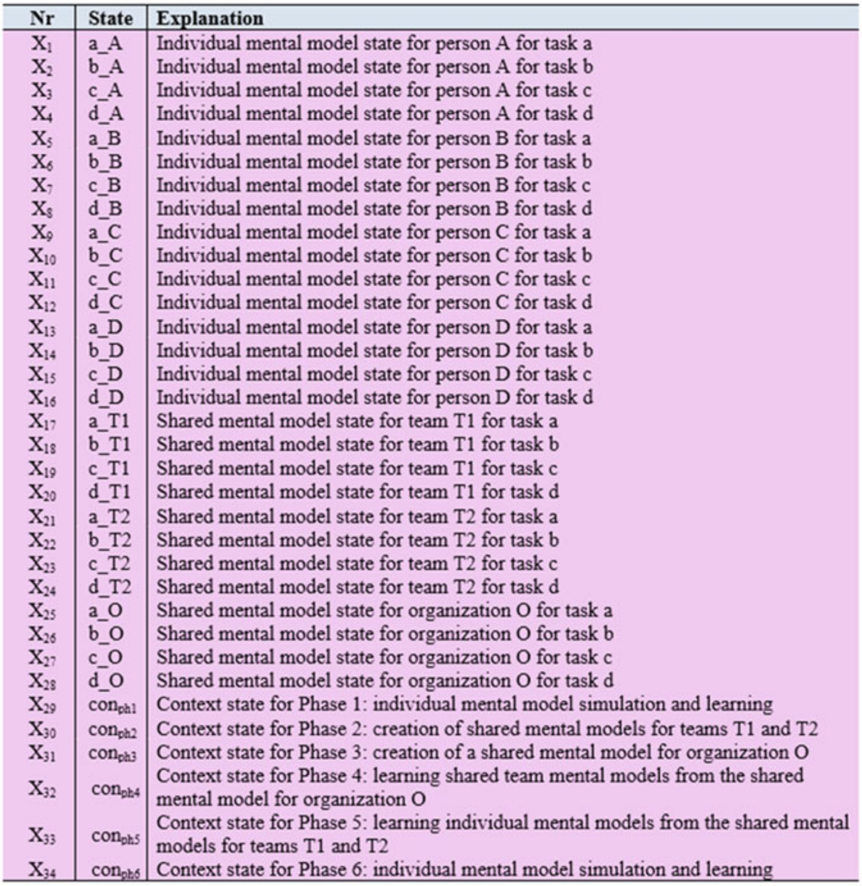
Fig. 3 Connectivity of the second-order adaptive network model for the second-order self-model of the mental models: the interactions between the first-order self-model level and the second-order self-model level: the second-order Hebbian learning for the second-order **W**-states (the $\mathbf{W_W}$-states)

is formalized computationally in the form of a self-modeling network architecture. In Bhalwankar and Treur [2], it is shown how specific forms of learning and their control can be modeled based on this self-modeling network architecture, in particular learning by observation and learning by instruction and combinations thereof Yi and Davis [16], Van Gog et al. [12]. Some of these forms of learning will also be applied in the model for multilevel organizational learning introduced here in Sect. 4.

4 The Network Model for Organizational Learning

In the considered case study concerning tasks *a*, *b*, *c*, and *d*, initially, the individual mental models of 4 people are different and based on some strong and some weak connections; they do not use a stronger shared mental model as that does not exist yet. The multilevel organizational learning addressed to improve the situation covers:

1. Individual (Hebbian) learning by persons of their mental models through internal simulation which results in stronger but still incomplete and different mental models. Person A and C's mental models have no connection from task *c* to task *d,* and person B and D's mental models have no connection from *a* to *b*.
2. Formation of two shared team mental models for teams T1 (consisting of persons A and B) and T2 (consisting of persons C and D) based on the different individual mental models. A process of unification by aggregation takes place (feed forward learning).



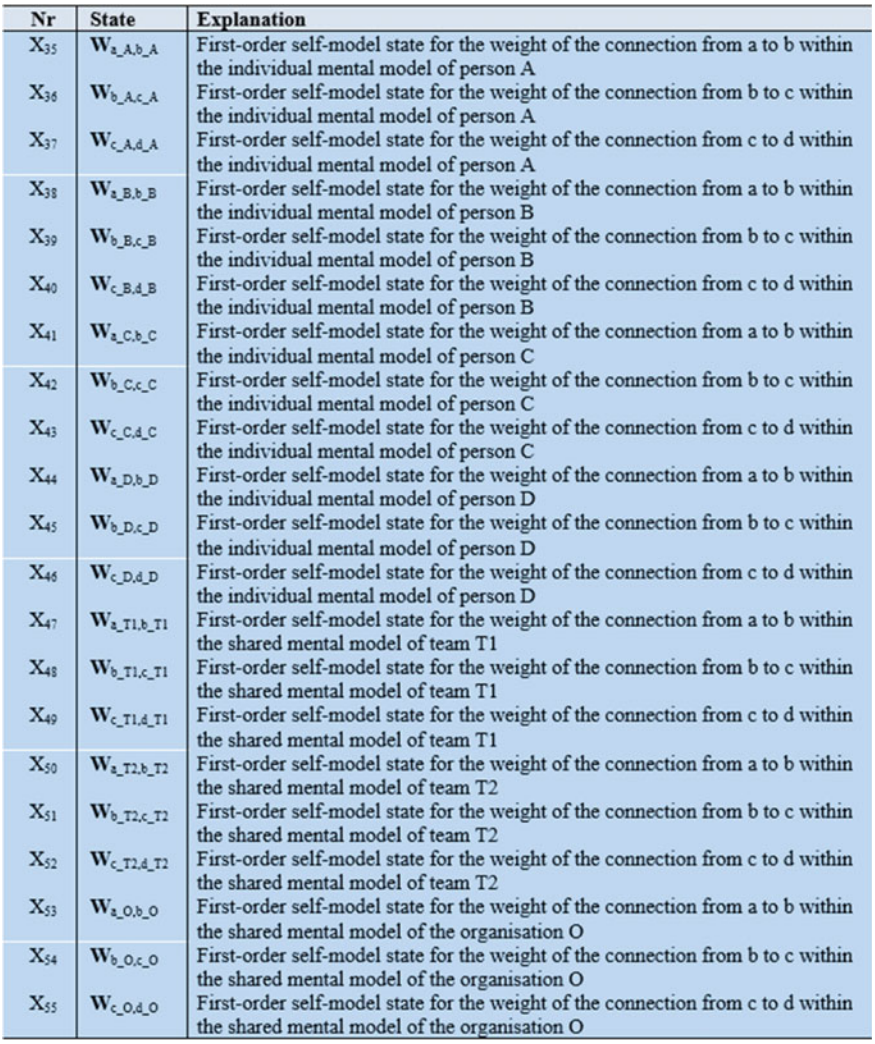
Nr	State	Explanation
X_1	a_A	Individual mental model state for person A for task a
X_2	b_A	Individual mental model state for person A for task b
X_3	c_A	Individual mental model state for person A for task c
X_4	d_A	Individual mental model state for person A for task d
X_5	a_B	Individual mental model state for person B for task a
X_6	b_B	Individual mental model state for person B for task b
X_7	c_B	Individual mental model state for person B for task c
X_8	d_B	Individual mental model state for person B for task d
X_9	a_C	Individual mental model state for person C for task a
X_{10}	b_C	Individual mental model state for person C for task b
X_{11}	c_C	Individual mental model state for person C for task c
X_{12}	d_C	Individual mental model state for person C for task d
X_{13}	a_D	Individual mental model state for person D for task a
X_{14}	b_D	Individual mental model state for person D for task b
X_{15}	c_D	Individual mental model state for person D for task c
X_{16}	d_D	Individual mental model state for person D for task d
X_{17}	a_T1	Shared mental model state for team T1 for task a
X_{18}	b_T1	Shared mental model state for team T1 for task b
X_{19}	c_T1	Shared mental model state for team T1 for task c
X_{20}	d_T1	Shared mental model state for team T1 for task d
X_{21}	a_T2	Shared mental model state for team T2 for task a
X_{22}	b_T2	Shared mental model state for team T2 for task b
X_{23}	c_T2	Shared mental model state for team T2 for task c
X_{24}	d_T2	Shared mental model state for team T2 for task d
X_{25}	a_O	Shared mental model state for organization O for task a
X_{26}	b_O	Shared mental model state for organization O for task b
X_{27}	c_O	Shared mental model state for organization O for task c
X_{28}	d_O	Shared mental model state for organization O for task d
X_{29}	con_{ph1}	Context state for Phase 1: individual mental model simulation and learning
X_{30}	con_{ph2}	Context state for Phase 2: creation of shared mental models for teams T1 and T2
X_{31}	con_{ph3}	Context state for Phase 3: creation of a shared mental model for organization O
X_{32}	con_{ph4}	Context state for Phase 4: learning shared team mental models from the shared mental model for organization O
X_{33}	con_{ph5}	Context state for Phase 5: learning individual mental models from the shared mental models for teams T1 and T2
X_{34}	con_{ph6}	Context state for Phase 6: individual mental model simulation and learning

Fig. 4 Base level states of the introduced adaptive network model

3. Formation of a shared organization mental model based on the two team mental models. Again, a process of unification by aggregation takes place (feed forward learning).
4. Flow of information and knowledge from organization mental model to team mental models, e.g., a form of instructional learning (feedback learning).
5. Learning of individual mental models from the shared team mental models, e.g., also a form of instructional learning (feedback learning).
6. Improvements on these individual mental models by individual learning through internal simulation which results in stronger and now complete mental models (by Hebbian learning). Now, person A and C’s mental models have a connection from task c to task d, and person B and D’s mental models have a connection from a to b.

The connectivity of the introduced network model is shown in Fig. 3; for an overview of the states, see Figs. 4 and 5, and for more details about the connections and how they relate to **(a)** to **(f)** from Sect. 2, see the Appendix stored as Linked Data at URL https://www.researchgate.net/publication/354352746.

The undermost base level of this model has mental model states for individuals, teams and organization, and also context states for activation of six different phases (like the **(a)** to **(f)** in Sect. 2.3) at different times. The mental states of persons are connected to each other according to the order of the tasks, and the first ones have a



Nr	State	Explanation
X_{35}	$\mathbf{W}_{a\_A,b\_A}$	First-order self-model state for the weight of the connection from a to b within the individual mental model of person A
X_{36}	$\mathbf{W}_{b\_A,c\_A}$	First-order self-model state for the weight of the connection from b to c within the individual mental model of person A
X_{37}	$\mathbf{W}_{c\_A,d\_A}$	First-order self-model state for the weight of the connection from c to d within the individual mental model of person A
X_{38}	$\mathbf{W}_{a\_B,b\_B}$	First-order self-model state for the weight of the connection from a to b within the individual mental model of person B
X_{39}	$\mathbf{W}_{b\_B,c\_B}$	First-order self-model state for the weight of the connection from b to c within the individual mental model of person B
X_{40}	$\mathbf{W}_{c\_B,d\_B}$	First-order self-model state for the weight of the connection from c to d within the individual mental model of person B
X_{41}	$\mathbf{W}_{a\_C,b\_C}$	First-order self-model state for the weight of the connection from a to b within the individual mental model of person C
X_{42}	$\mathbf{W}_{b\_C,c\_C}$	First-order self-model state for the weight of the connection from b to c within the individual mental model of person C
X_{43}	$\mathbf{W}_{c\_C,d\_C}$	First-order self-model state for the weight of the connection from c to d within the individual mental model of person C
X_{44}	$\mathbf{W}_{a\_D,b\_D}$	First-order self-model state for the weight of the connection from a to b within the individual mental model of person D
X_{45}	$\mathbf{W}_{b\_D,c\_D}$	First-order self-model state for the weight of the connection from b to c within the individual mental model of person D
X_{46}	$\mathbf{W}_{c\_D,d\_D}$	First-order self-model state for the weight of the connection from c to d within the individual mental model of person D
X_{47}	$\mathbf{W}_{a\_T1,b\_T1}$	First-order self-model state for the weight of the connection from a to b within the shared mental model of team T1
X_{48}	$\mathbf{W}_{b\_T1,c\_T1}$	First-order self-model state for the weight of the connection from b to c within the shared mental model of team T1
X_{49}	$\mathbf{W}_{c\_T1,d\_T1}$	First-order self-model state for the weight of the connection from c to d within the shared mental model of team T1
X_{50}	$\mathbf{W}_{a\_T2,b\_T2}$	First-order self-model state for the weight of the connection from a to b within the shared mental model of team T2
X_{51}	$\mathbf{W}_{b\_T2,c\_T2}$	First-order self-model state for the weight of the connection from b to c within the shared mental model of team T2
X_{52}	$\mathbf{W}_{c\_T2,d\_T2}$	First-order self-model state for the weight of the connection from c to d within the shared mental model of team T2
X_{53}	$\mathbf{W}_{a\_O,b\_O}$	First-order self-model state for the weight of the connection from a to b within the shared mental model of the organisation O
X_{54}	$\mathbf{W}_{b\_O,c\_O}$	First-order self-model state for the weight of the connection from b to c within the shared mental model of the organisation O
X_{55}	$\mathbf{W}_{c\_O,d\_O}$	First-order self-model state for the weight of the connection from c to d within the shared mental model of the organisation O

Fig. 5 First-order self-model states of the introduced adaptive network model

connection from first context state to be able to start to perform internal simulation and learn. As can be seen in Fig. 3, some connections between task states of persons are dashed, which means initially there is no connection. Therefore, states where these dashed connections are, are the "hollow" non-known mental states of persons. These states have connections from a fifth context state to enable to observe the improvement of individual with the impact of organization and team mental models in Phase 5. The base level mental states relate to the basic tasks and can be considered as the basic ingredients of the mental models representing knowledge on relations between tasks.

To make the mental models adaptive, first-order self-model states are added in the intermediary level. These are **W**-states representing adaptive weights for each developed connection of individual, team, and organization mental states in the base level. There are also intralevel **W**-to-**W** connections between first-order **W**-states here to provide feed forward learning in Phase 2 and Phase 3 and feedback learning in Phase 4 and Phase 5 [5]. These **W**-to-**W** connections correspond to the arrows for feed forward and feedback learning shown in Fig. 1.

Formation of shared team and organization mental models is performed by this feed forward learning mechanism, and the learning from the shared organization mental model and the shared team mental model by individuals occurs by the feedback learning mechanism.

To control this adaptivity in first-order adaptation level, second-order self-model states are added in the uppermost level. In first place, there are $\mathbf{W}_{\mathbf{W}}$-states (higher-order **W**-states) for (intralevel) connections between first-order adaptivity level **W**-states, in other words, adaptive weight representation of the connections of adaptive weight representation states in the level below. These control processes are left out of consideration in Fig. 1 based on Crossan et al. [5] and Wiewiora et al. [15] but still are crucial for the processes to function well. Additionally, $\mathbf{H}_{\mathbf{W}}$-states for adaptation speeds of connection weights in the first-order adaptation level and $\mathbf{M}_{\mathbf{W}}$-states for persistence of adaptation are placed here. This provides the speed and persistence control of the adaptation. For a full specification of the network model, see linked data at https://www.researchgate.net/publication/354352746.

5 Example Simulation Scenario

In this scenario, for reasons of presentation, a multi-phase approach is applied to get a clear picture of the progress of multilevel organizational learning via teams. In general, the model can also process all phases simultaneously. It is possible to see the feed forward flow of the development of shared team mental models from individual mental models first, formation of the shared organization mental model originating from teams' mental models, then and finally, by the feedback flow, the impact of these shared mental models on teams and individuals. In practice and also in the model, these phases also can overlap or take place entirely simultaneously. The considered six phases are as follows:

- **Phase 1**: **Individual mental model usage and learning**

This relates to **(a)** in Sect. 2. Different individual mental models by four different persons are constructed and strengthened here. The knowledge levels of people for the tasks, initially, are not same. Thus, the learning levels are different as can be seen in the first phase between time 25 and 200 in the simulation graph in Fig. 6. For example, activation levels of first three base state for tasks *a* to *c* of person A from Team 1 and person C from Team 2 (a_A to c_A and a_C to c_C) increase while the activation levels of states for task *d* (d_A and d_C) remain at zero indicating that they do not have knowledge on this task. A similar lack of knowledge is observed for the other persons B from Team 1 and D from Team 2, for task *a* this time. Therefore, the activation levels of their states a_B and a_D remain at zero in this phase, while others get increased (b_B to d_B and b_D to d_D). After this first individual learning phase, forgetting takes place for all persons because they do not have perfect persistence factors self-model **M**-state values (values < 1, meaning imperfection). Increased

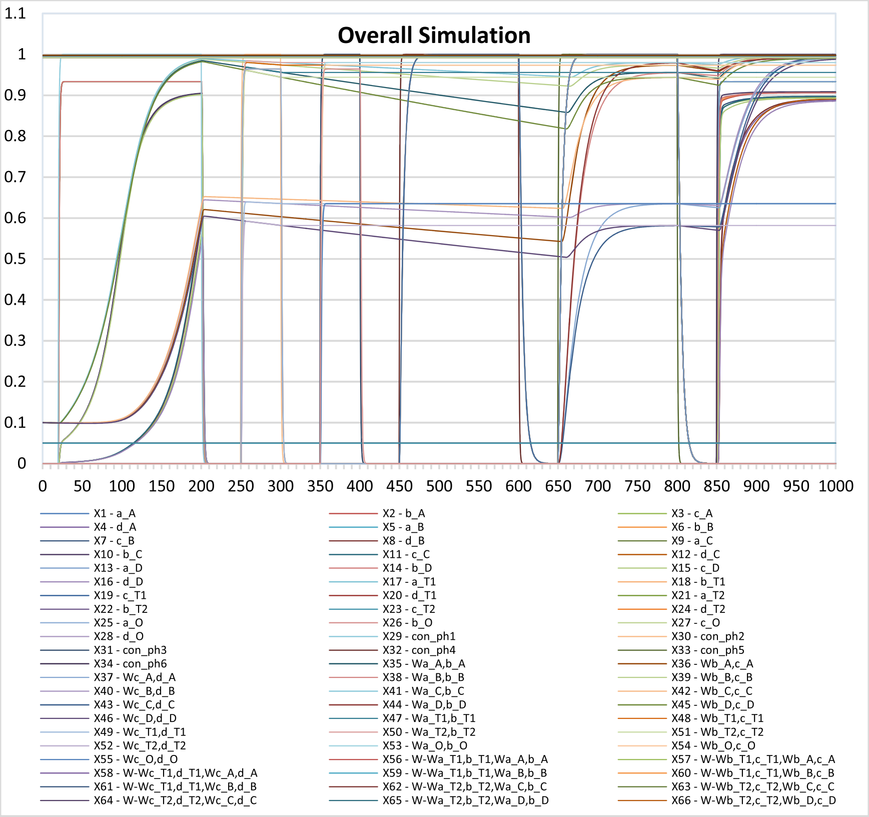


Fig. 6 Simulation graph showing all states

W-states during phase 1, start to slightly decrease after phase 1 at different rates representing the differences between persons concerning forgetting speed.

- **Phase 2: Shared team mental model formation (feed forward learning)**

This relates to **(b)** in Sect. 2. Formation of two shared team mental models happens in this phase. The collaboration of the individuals creates the aggregation of their mental models as part of feed forward organizational learning (in this case team learning). The **W**-states of the teams ($\mathbf{W}_{\text{a\_T1,b\_T1}}$ to $\mathbf{W}_{\text{c\_T1,d\_T1}}$ and $\mathbf{W}_{\text{a\_T2,b\_T2}}$ to $\mathbf{W}_{\text{c\_T2,d\_T2}}$) increase at different rates in Phase 2 between time 250 and 300 in Fig. 6. Team 1 becomes better at the connection *c*→*d,* and Team 2 becomes better at connection *a*→*b* because the teams have different persons. Then, these shared mental models are maintained by the two teams.

- **Phase 3: Shared organization mental model formation (feed forward learning)**

This relates to **(c)** in Sect. 2. A shared organization mental model is formed in this phase from the unification and aggregation of the two shared team mental models. The values of shared organization mental model **W**-states ($\mathbf{W}_{\text{a\_O,b\_O}}$ to $\mathbf{W}_{\text{c\_O,d\_O}}$) increase here between time 350 and 400.

- **Phase 4: Feedback learning of the shared team mental model from the shared organization mental model**

This relates to **(d)** in Sect. 2. Knowledge from the shared organization mental model is received by the team mental models as a form of (instructional) feedback learning here in this phase. The (higher-order adaptive) connections from organization **W**-states to teams **W**-states (X_{68} to X_{73}) become activated, and the teams start to get stronger connections about tasks.

- **Phase 5: Feedback learning of the individual mental models from the shared team mental models**

This relates to **(e)** in Sect. 2. Improved knowledge from shared team mental models is received by individuals as a form of (instructional) feedback learning in this phase. Higher-order adaptive weight states for connections from teams **W**-states to individual **W**-states (X_{56} to X_{67}) are activated. This provides the learning of individual mental models and gives persons the chance of improving their unknown connections in the next phase. For instance, the person A starts to learn about the task *d* that it does not know in the beginning by the help of its team. In Fig. 6, the **W**-states of persons make jumps in this Phase 5 between time 650 and 800.

- **Phase 6: Individual mental model usage and learning**

This relates to **(f)** in Sect. 2. Persons start to further improve their knowledge and skills (their mental models) already strengthened in Phase 5 by Hebbian learning [6]. Person A's knowledge on task *d* (state d_A) becomes nonzero now (obtained via shared team mental model), and similar improvements are observed for other persons and their “hollow” unknown states.

6 Discussion

Within mainstream organizational learning literature such as Crossan et al. [5], Wiewiora et al. [15], mental models at individual, team, and organization levels and the interplay of them are considered to be a vehicle for organizational learning. This is called multilevel organizational learning. Based on developed individual mental models, by socalled feed forward learning, the formation of shared team mental models can take place and based on them, a shared mental model for the level of the organization as a whole (see also Fig. 1 adopted from the mentioned literature). Once these shared mental models have been formed, they can be adopted by individuals within the organization, indicated as feedback learning. This involves a number of mechanisms of different types that by their cyclical interaction together can be considered to form the basis of multilevel organizational learning. These mechanisms have been formalized in a computational manner here and brought together in an adaptive self-modeling network architecture. The model was illustrated by a relatively simple but realistic case study. For the sake of presentation, in the case study scenario, the different types of mechanisms have been controlled in such a manner that they are sequentially over time. This is not inherent in the designed computational network model: these processes can equally well work simultaneously. The two lowest levels of the three-level network model describe Fig. 1 very well, especially the intralevel connections within the middle level directly correspond to the arrows in Fig. 1. However, the necessary control of these processes is left out of consideration in Fig. 1 but is fully addressed here by the highest (third) level. For many more details about this modeling approach for multilevel organisational learning, see also the forthcoming book [4].

One of the extension possibilities concerns the type of aggregation used for the process of shared mental model formation. In the current model, this has been based on the maximal knowledge about a specific mental model connection. But other forms of aggregation can equally well be applied, for example, weighted averages. Another possible extension is to make states used for the control adaptive in a context-sensitive manner, such as the second-order self-model **H**- and **M**-states for the individuals, which for the sake of simplicity were kept constant in the current example scenario.

References

1. Argyris C, Schön DA (1978) Organizational learning: a theory of action perspective. Addison-Wesley, Reading, MA

2. Bhalwankar R, Treur J (2021) Modeling learner-controlled mental model learning processes by a second-order adaptive network model. PLoS One 16(8):e0255503
3. Bogenrieder I (2002) Social architecture as a prerequisite for organizational learning. Manag Learn 33(2):197–216
4. Canbaloğlu G, Treur J, Wiewiora A (eds) (2023) Computational modeling of multilevel organisational learning and its control using self-modeling network models (to appear). Springer Nature
5. Crossan MM, Lane HW, White RE (1999) An organizational learning framework: from intuition to institution. Acad Manag Rev 24:522–537
6. Hebb DO (1949) The organization of behavior: a neuropsychological theory. Wiley, New York
7. Kim DH (1993) The link between individual and organisational learning. Sloan Manag Rev 1993:37–50
8. McShane SL, von Glinow MA (2010) Organizational behavior. McGraw-Hill (2010)
9. Stelmaszczyk M (2016) Relationship between individual and organizational learning: mediating role of team learning. J Econ Manag 26(4):1732–1947. https://doi.org/10.22367/jem.2016.26.06
10. Treur J (2020) Network-oriented modeling for adaptive networks: designing higher-order adaptive biological, mental and social network models. Springer Nature, Cham
11. Treur J, Van Ments L (eds) (2022) Mental models and their dynamics, adaptation, and control: a self-modeling network modeling approach. Cham Switzerland, Springer Nature
12. Van Gog T, Paas F, Marcus N, Ayres P, Sweller J (2009) The mirror neuron system and observational learning: implications for the effectiveness of dynamic visualizations. Educ Psychol Rev 21(1):21–30
13. Van Ments L, Treur J, Klein J, Roelofsma PHMP (2021) A second-order adaptive network model for shared mental models in hospital teamwork. In: Proceedings of ICCCI'21. Lecture Notes in AI, vol 12876. Springer Nature, pp 126–140
14. Wiewiora A, Chang A, Smidt M (2020) Individual, project and organizational learning flows within a global project-based organization: exploring what, how and who. Int J Project Manage 38:201–214
15. Wiewiora A, Smidt M, Chang A (2019) The 'How' of multilevel learning dynamics: a systematic literature review exploring how mechanisms bridge learning between individuals, teams/projects and the organization. Eur Manag Rev 16:93–115
16. Yi MY, Davis FD (2003) Developing and validating an observational learning model of computer software training and skill acquisition. Infor Syst Res 14(2):146–169

A Novel Video Prediction Algorithm Based on Robust Spatiotemporal Convolutional Long Short-Term Memory (Robust-ST-ConvLSTM)

Wael Saideni, David Helbert, Fabien Courreges, and Jean Pierre Cances

Abstract Recently, video prediction algorithms based on neural networks have become a promising research direction. Therefore, a new recurrent video prediction algorithm called "Robust Spatiotemporal Convolutional Long Short-Term Memory" (Robust-ST-ConvLSTM) is proposed in this paper. Robust-ST-ConvLSTM proposes a new internal mechanism that is able to regulate efficiently the flow of spatiotemporal information from video signals based on higher-order Convolutional-LSTM. The spatiotemporal information is carried through the entire network to optimize and control the prediction potential of the ConvLSTM cell. In addition, in traditional ConvLSTM units, cell states, that carry relevant information throughout the processing of the input sequence, are updated using only one previous hidden state, which holds information on previous data unit already seen by the network. However, our Robust-ST-ConvLSTM unit will rely on N previous hidden states, that provide temporal context for the motion in video scenes, in the cell state updating process. Experimental results further suggest that the proposed architecture can improve the state-of-the-art video prediction methods significantly on two challenging datasets, including the standard Moving MNIST dataset, and the commonly used video prediction KTH dataset, as human motion dataset.

Keywords Video prediction · Deep learning · Neural networks · Computer vision · ConvLSTM · Memory flow · Hidden states

W. Saideni (✉) · D. Helbert · F. Courreges · J. P. Cances
XLIM Research Institute, UMR CNRS 7252, Limoges, France
e-mail: wael.saideni@xlim.fr

D. Helbert
e-mail: david.helbert@univ-poitiers.fr

F. Courreges
e-mail: fabien.courreges@unilim.fr

J. P. Cances
e-mail: cances@ensil.unilim.fr

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_17

1 Introduction

Video prediction, one of the emerging fields of computer vision, is facing several challenges [1–5]. Actually, it has gained significant interests due to its broad-ranging realistic forecasting applications, such as traffic flow prediction and video surveillance.

The great progress made by deep learning in a wide range of applications and research fields, motivated authors to explore deep learning architectures to predict future video frames. The main advantage of deep learning models is their potential to learn adequate features from high-dimensional data, such as videos, in an end-to-end manner without hand-designed features [6]. However, despite the significant progress in deep learning architectures, video prediction is still considered as a big challenge, especially in terms of output visual quality and long-term prediction. Therefore, our Robust Spatiotemporal Convolutional Long Short-Term Memory (Robust-ST-ConvLSTM) algorithm is proposed as a long-term prediction algorithm that outperforms the state-of-the-art approaches in terms of quality performances. Our algorithm is based on a modified version of ConvLSTM cell. Obviously, ConvLSTM is not very efficient in handling long sequences. Indeed, ConvLSTM-based algorithms focus on stochastic features of the data rather than its spatial distortion. Also, a temporal information encoding in ConvLSTM unit [7] is based on first-order Markovian architecture. Thus, making long-range temporal correlations hard to extract. In addition, the vanishing gradient problem often occurs in training first-order RNN-based predictive algorithms [8].

Bearing all these drawbacks in mind, we propose our Robust-ST-ConvLSTM algorithm for video prediction. With the following properties, we hope our algorithm will pave the way for the application of recurrent neural network on real-wold datasets:

- Spatial and temporal data are taken into consideration jointly.
- The new spatiotemporal memory (STM) cell transfers low-level and semantic aspects of the dynamic scene which are the key of generating future frames.
- The Robust-ST-ConvLSTM new internal mechanism offers new cell state and hidden state transition functions to efficiently regulate the flow of spatiotemporal information from the input videos.
- The algorithm aims to rely on N previous hidden states, that provide temporal context for the motion in video scenes, to update one cell state at every timestep.

The remainder of this paper is organized as follows: The related works on video prediction are discussed in Sect. 2. In Sect. 3, our proposed Robust-ST-ConvLSTM algorithm is presented. Sect. 4 provides the experimental results. Sect. 5 concludes the paper.

2 Related Works

Video prediction algorithms have used various deep learning architectures to enhance the quality performance of the predicted frames and to fasten the process. Deep learning has been extensively used to analyze the frames and extract their features exploited in spatiotemporal predictive learning.

Recent deep learning approaches can be categorized into three classes: recurrent neural approaches, convolutional networks-based algorithms, and generative networks.

Recurrent neural networks (RNN) have demonstrated a significant success in recent video prediction-related works [9–25]. ConvLSTM [7] is considered as a crucial branch in predicting future frame. A two-stream architecture based on adversarial training to model deterministic dynamics is proposed by Zhang et al. [12]. It enables to update hidden states along a z-order curve. Wang et al. [26] proposed PredRNN as a sequence of recurrent blocks defining an additional global memory cell in order to ameliorate the prediction ability of the network. However, the proposed memory cell transfers long-term and short-term data at the same time which can restrict the predictive performances of the network. Therefore, a pair of memory cell is introduced in [27] and explicitly decoupled to deal with different variations. Also, reverse scheduled sampling strategy was added to learn temporal dynamics and reduce the training discrepancy between the encoding and the prediction structures.

Convolutional networks, considered as feed-forward neural networks, are also commonly used in the future prediction problems. A multi-model is defined in [28] to model dynamic patterns and learn image representation by combining temporal and spatial sub-networks. In [29], Deep Voxel Flow (DVF) is trained to synthesize future frames by flowing pixel values directly from input frames. It can predict the in-between frames (interpolation) and the future frames (extrapolation) of the input video. Another interesting convolutional networks for video prediction are 3D convolutions-based models to capture temporal consistency [30–33].

Generative networks are used to synthesize new frames by learning a probability distribution from the input data. Generative Adversarial Networks (GAN) [34] are commonly used in video prediction architectures. Kwon et al. [35] proposed a retrospective cycle GAN-based algorithm to predict video frames. In [36], it is confirmed that conditional Generative Adversarial Networks (cGAN) can ensure the spatiotemporal coherence between the input videos and the generated frames. Designing a network by dividing the video data into content part and motion part is discussed in [37]. The content part detects the objects in the sequence and the motion part captures their movements. This video prediction framework introduces a new adversarial learning scheme.

3 The Proposed Robust Spatiotemporal ConvLSTM Architecture

Our algorithm is based on Robust Spatiotemporal Convolutional Long Short-Term Memory (Robust-ST-ConvLSTM) cell that is an extended version of ConvLSTM cell.

3.1 Convolutional Long Short-Term Memory (ConvLSTM)

ConvLSTM is considered as a Long Short-Term Memory (LSTM) [38] network applied on high-dimensional data. In fact, LSTM is a powerful network commonly used to solve time series problems thanks to its ability to avoid long-term dependency problems and remember information for long periods of time. Its main structure enables to connect previous information to the future function. However, LSTM is inadequate to process high-dimensional data since it requires 1D vectors as input. Therefore, ConvLSTM was proposed to extract spatial features for the prediction mode. Different from LSTM unit, ConvLSTM cell structure is based on 3D tensors, including the inputs X_t, the cell states C_t, and the hidden states H_t.

3.2 The Proposed Robust Spatiotemporal ConvLSTM Algorithm

Robust Spatiotemporal ConvLSTM (Robust-ST-ConvLSTM) algorithm shows a new internal mechanism that is able to regulate efficiently the flow of spatiotemporal information from video signals based on higher-order Convolutional-LSTM. The proposed algorithm decides the cell state C_t from N previous hidden states (H_{t-2}, ..., H_{t-N}). N will be fixed by the user depending on the application, the reconstruction quality required and the computational resources available. The proposed Robust-ST-ConvLSTM requires also to implement a memory flow to hold the spatiotemporal information in order to optimize and control the prediction abilities of ConvLSTM. Indeed, the memory flow will be a second cell state to handle spatiotemporal data since the cell state C_t handles temporal data and will not be eliminated. Robust-ST-ConvLSTM uses a stack of ConvLSTM units to learn spatial correlations and temporal dynamics from the input scene. These features will be used to predict the future frames. Thus, a novel transition function is defined based on spatiotemporal memory flow to support previous hidden states.

The process of updating temporal cell states C_t, in ConvLSTM, is activated from one timestep to another. However, successive frames have temporal correlations and very close spatial data distribution. Hence, these properties can be exploited to make better predictions. Therefore, Robust-ST-ConvLSTM, considered as a higher-order ConvLSTM based on memory flow, will exploit the global motion changes of the consecutive frames and the spatiotemporal memory information to forecast future frames. An horizontal diagram flow can represent the memory state updating process for the original stacked ConvLSTM. We suggest here to upgrade the previous model by updating the memory state horizontally (cell state C_t) and also vertically (spatiotemporal memory state STM_t) as shown in Fig. 1. This process will enhance the way spatiotemporal information is handled from the input to the output and allow to connect all the recurrent units of the entire network.

From a mathematical perspective, the new robust spatiotemporal unit, illustrated in Fig. 2, can be defined as:

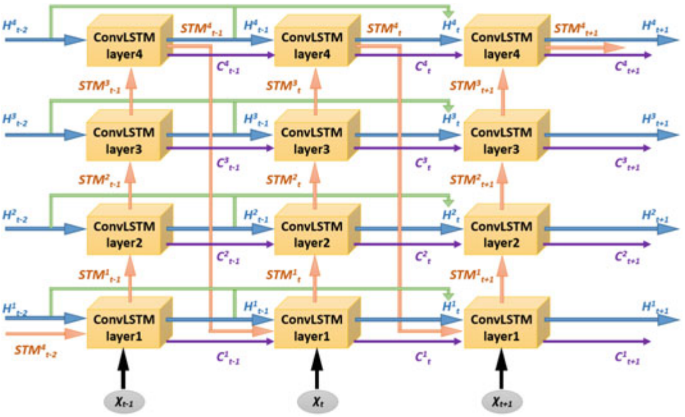


Fig. 1 Main structure of robust spatiotemporal LSTM

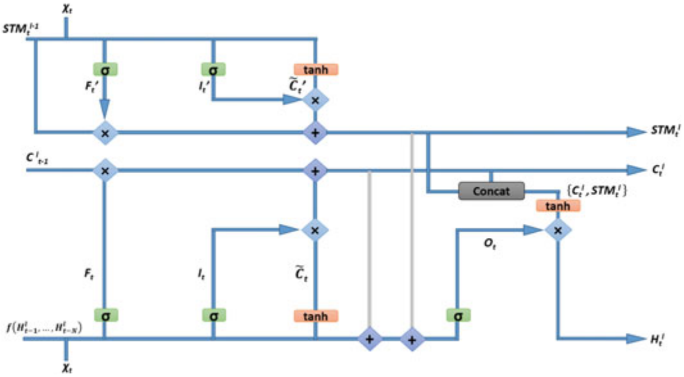


Fig. 2 Robust spatiotemporal unit

$$\begin{aligned}
I_t &= \sigma(W_i * X_t + f(H^l_{t-1}, ..., H^l_{t-N})) \\
F_t &= \sigma(W_f * X_t + f(H^l_{t-1}, ..., H^l_{t-N})) \\
\hat{C}_t &= tanh(W_{\hat{c}} * X_t + f(H^l_{t-1}, ..., H^l_{t-N})) \\
C^l_t &= F_t \circ C^l_{t-1} + I_t \circ \hat{C}_t \\
I'_t &= \sigma(W'_i * X_t + M'_i * STM^{l-1}_t) \\
F'_t &= \sigma(W'_f * X_t + M'_f * STM^{l-1}_t) \\
\hat{C}'_t &= tanh(W'_{\hat{c}} * X_t + M'_{\hat{c}} * STM^{l-1}_t) \\
STM^l_t &= F'_t \circ STM^{l-1}_t + I'_t \circ \hat{C}'_t \\
O_t &= \sigma(W_{ox} * X_t + f(H^l_{t-1}, ..., H^l_{t-N}) \\
&\quad + W_{oc} * C^l_t + W_{ostm} * \mathrm{STM}^l_t) \\
H^l_t &= O_t * tanh(W_{1\times 1} * [C^l_t, \mathrm{STM}^l_t])
\end{aligned} \tag{1}$$

Where σ is the sigmoid activation function, $*$ and $\circ$ represent the convolution operator and the Hadamard product, respectively. Same as ConvLSTM structure, I_t and I'_t denote the input gates, F_t and F'_t symbolize the forget gates, $\hat{C}_t$ and $\hat{C}'_t$ represent the potential cell states, O_t denotes the output gate. X_t represents the input at the time step t. H^l_t symbolizes the hidden state of the lth layer at the time step t. C^l_t is the memory state of the lth layer at the time step t. STM^l_t represents the spatiotemporal memory of the lth layer at the time step t. f denotes the function combining N previous hidden states.

The design of the function f must satisfy the following conditions:

- Hidden states have a spatial structure that should be preserved.
- To capture the context of the previous frames (timesteps), the size of the filters controlling the previous hidden states structure should increase over timesteps.
- Computational complexity does not have to explode.

In order to implement *f*, our approach is inspired from recursive least-squares filters used in signal processing [39]. Indeed, the idea is to focus on returning the mean value of all elements in the input tensor that handle the previous hidden states. In Robust-ST-ConvLSTM, combining multiple preceding hidden states generates a feedback signal. Then, the state of the N-order Robust-St-ConvLSTM is recursively updated with the following function f:

$$f(H^l_{t-1}, ..., H^l_{t-N}) = \frac{1}{N}\sum_{n=1}^{N} \alpha^n_n W_{hn} H^l_{t-n} \tag{2}$$

where α denotes the forgetting factor. The parameter α $(0 < \alpha < 1)$ gives more weight to recent hidden states.

Unlike ConvLSTM-based architectures, robust spatiotemporal unit depends on the previous hidden states from the previous timesteps at the same layer and the spatiotemporal memory state. Precisely, the first layer in a stacked ConvLSTM model at time step t receives the spatiotemporal memory of the last layer in the stacked model of the previous time step as illustrated in Fig. 1 ($STM^1_t = STM^L_{t-1}$ with L is the number of stacked layers).

Consequently, the main structure of ConvLSTM has been modified by adding a second gated structure for the spatiotemporal memory STM_t^1. Yet, the final hidden state H_t^l depends on the fusion of the spatiotemporal memory state STM_t^l and the temporal memory state C_t^l.

The spatiotemporal memory is implemented to reduce the loss of spatiotemporal information in multidimensional data from the top layer to the bottom layer of the network. Moreover, previous hidden states, used as input, are implemented to enlarge the visibility of the neural units about the context of the ongoing events at different timesteps.

In comparison with standard ConvLSTM model, our proposed approach increases the number of parameters, especially with the addition of a second gated structure. However, it prevents an unnecessarily expenditure of ConvLSTM model (by adding some hyperparameters) to obtain the same performances.

4 Experiments

4.1 *Datasets and Performance Metrics*

Robust-ST-ConvLSTM architecture is tested on two motion video datasets: KTH [40] for human motion and Moving MNIST [41]. To compare its performances with the state-of-the-art approaches, frames quality evaluation metrics are used. Those metrics are peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM) [42].

4.2 *Implementation Details of Robust-ST-ConvLSTM*

Python 3.6 is used to implement the proposed architecture. For its ability to store and process multidimensional data, Pytorch 1.4.0 is used to develop the deep learning framework.

Adam optimizer [43] is used as an optimization algorithm to minimize the loss function with a learning rate of 0.0001. We choose a mini-batch of 2 sequences at each training iteration. We put an end to the training process after 100.000 iterations. As illustrated in Fig. 1, our proposed architecture is composed of 4 stacked ConvLSTM layers for each timestep. Three hidden states are used to enhance the prediction process and our model becomes a third-order Robust-ST-ConvLSTM. The dimensions of the hidden state depend on the input frames.

We train our implementation on the RTX 2060 GPU. It takes about a week to train the entire network on KTH dataset and about 4 days on Moving MNIST.

Table 1 Quantitative evaluation of different algorithms on the KTH dataset

Model	PSNR(dB)	SSIM
ConvLSTM [25]	23.009	0.704
PredRNN [26]	27.624	0.839
PredRNN [27]	28.502	0.831
Robust-ST-ConvLSTM	**28.992**	**0.854**

The metrics are averaged over the 20 predicted frames

4.3 Comparisons with the State-of-the-Art Methods

Quantitative results of the proposed algorithm and state-of-the-art networks on KTH dataset are illustrated in Table 1. Table 1 summarizes the comparisons with previous methods on PSNR and SSIM. The corresponding frame-wise comparisons are presented in Fig. 3 and Fig. 4. It can be observed that our proposed Robust-ST-ConvLSTM for video prediction outperforms the others. It increases the average PSNR and SSIM over the same number of predicted frames by 26% and 21.31%, respectively, in comparison with standard ConvLSTM-based method. Also, Robust-ST-ConvLSTM performs favorably against PredRNN-v2017 [26] and PredRNN-v2021 [27]. It performs better than PredRNN-v2021 by 1.72% and 2.77% in terms of PSNR and SSIM, respectively. The efficiency of our proposed approach in forecasting future frames in a video is proved by the qualitative results. Figure 5 plots the generated frames of different methods compared with the ground truth. Robust-ST-ConvLSTM provides clearer and sharper prediction than other approaches. Details are predicted accurately because of the memory flow which enhances the long-term prediction ability of the ConvLSTM cell.

Furthermore, the qualitative evaluation of our Robust-St-ConvLSTM and the state-of-the-art algorithms on Moving MNIST dataset by predicting 10 frames based on the features of the previous 10 input frames is illustrated in Table 2.

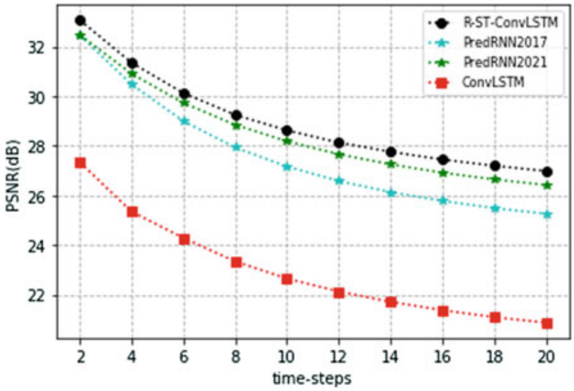


Fig. 3 Frame-wise PSNR comparisons of different models on KTH dataset after 100,000 iterations

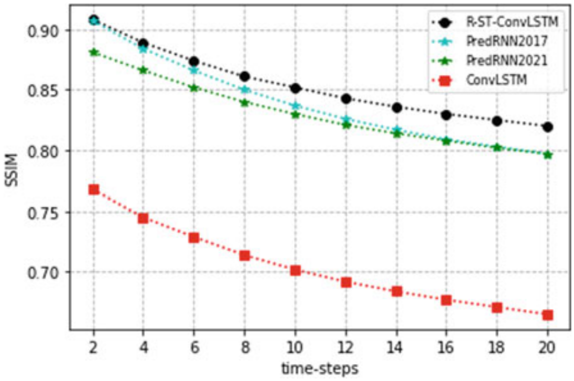


Fig. 4 Frame-wise SSIM comparisons of different models on KTH dataset after 100,000 iterations

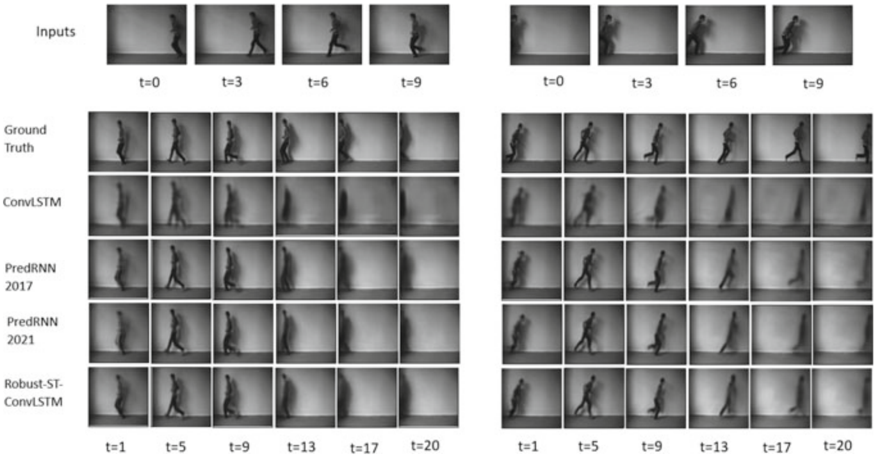


Fig. 5 Prediction examples on the KTH data set, where we predict 20 frames into the future based on the past 10 frames

As presented in Table 2, our proposed model outperforms the state-of-the-art approaches in both metrics, thus confirming the previous observations on KTH dataset. Our model increases the average PNSR over the 10 predicted frames by 3.15% by comparing it with PredRNN-v2021. In terms of SSIM, our Robust-ST-ConvLSTM outperforms PredRNN-v2021 by 0.22%. Also, compared with the standard ConvLSTM based model, our proposed algorithm has better PSNR ($\geq$14.59%) and SSIM ($\geq$26.95%) performances.

In this research work, various values of α have been tested randomly ($0 < \alpha < 1$) and the optimum value was selected for the comparison ($\alpha = 0.9$). This means that determining the optimal value of α could be an interesting research direction. Previous observations about the value of α and the number of hidden states

Table 2 Quantitative evaluation of different algorithms on the MNIST dataset

Model	PSNR(dB)	SSIM
ConvLSTM [25]	28.380	0.705
PredRNN [26]	30.569	0.869
PredRNN [27]	31.525	0.893
Robust-ST-ConvLSTM	**32.520**	**0.895**

The metrics are averaged over the 10 predicted frames

confirm that a trade-off should be done between quality performances and computational cost, in the future research work, to enhance the quality performances of the predicted images without training a computationally expensive algorithm.

5 Conclusion

In this paper, we present a new recurrent neural network model for predicting future video frames named "Robust Spatiotemporal ConvLSTM" (Robust-ST-ConvLSTM). It is based on a new robust spatiotemporal unit, an extension architecture of ConvLSTM. Our approach learns extra information from the memory flow that handles the spatiotemporal information to significantly improve the long-term frame prediction. We further improve the temporal context for the motion in videos by opting for a higher-order ConvLSTM approach to enable cell states update from previous hidden states. Qualitative and quantitative results demonstrate the superiority of our algorithm dealing with video prediction, showing state-of-the-art performance in KTH and Moving MNIST datasets. This architecture inspires us to further explore recurrent structures to optimize the computational cost of the algorithm and generate accurate predictions in the future research work.

Acknowledgements This work was supported in part by the sensors generation project of Nouvelle Aquitaine region (2018-1R50214).

References

1. Kitani KM, Ziebart BD, Bagnell JA, Hebert M (2012) Activity forecasting. In: ECCV
2. Vondrick C, Pirsiavash H, Torralba A (2016) Anticipating visual representations from unlabeled video. In: CVPR
3. Zeng K, Shen WB, Huang D, Sun M, Niebles JC (2017) Visual forecasting by imitating dynamics in natural sequences. In: ICCV
4. Bhattacharyya A, Fritz M, Schiele B (2018) Long-term on-board prediction of people in traffic scenes under uncertainty. In: CVPR
5. Hu A, Cotter F, Mohan N, Gurau C, Kendall A (2020) Probabilistic future prediction for video scene understanding. arXiv:2003.06409

6. LeCun Y, Bengio Y, Hinton GE (2015) Deep learning. Nature 521(7553)
7. Xingjian S et al (2015) Convolutional LSTM network: a machine learning approach for precipitation nowcasting,. In: Proceedings of advanced neural information processing systems, pp 802–810
8. Soltani R, Jiang H (2016) Higher order recurrent neural networks. arXiv:1605.00064
9. Lotter W, Kreiman G, Cox DD (2015) Unsupervised learning of visual structure using predictive generative networks. arXiv:1511.06380
10. Wichers N, Villegas R, Erhan D, Lee H (2018) Hierarchical long-term video prediction without supervision. In: ICML, Series proceedings of machine learning research, vol 80
11. Villegas R, Yang J, Zou Y, Sohn S, Lin X, Lee H (2017) Learning to generate long-term future via hierarchical prediction. In: ICML
12. Zhang J, Wang Y, Long M, Jianmin W, Yu PS (2019) Z-order recurrent neural networks for video prediction. In: ICME
13. Ranzato M, Szlam A, Bruna J, Mathieu M, Collobert R, Chopra S (2014) Video (language) modeling: a baseline for generative models of natural videos. arXiv:1412.6604
14. Srivastava N, Mansimov E, Salakhutdinov R (2015) Unsupervised learning of video representations using LSTMs. In: ICML
15. Lotter W, Kreiman G, Cox D (2017) Deep predictive coding networks for video prediction and unsupervised learning. In: ICLR (Poster)
16. Byeon W, Wang Q, Srivastava RK, Koumoutsakos P (2018) Contextvp: fully context-aware video prediction. In: CVPR (Workshops)
17. Patraucean V, Handa A, Cipolla R (2015) Spatio-temporal video autoencoder with differentiable memory. In: (ICLR) workshop
18. Lu C, Hirsch M, Scholkopf B (2017) Flexible Spatio-temporal networks for video prediction. In: CVPR
19. Denton EL, Birodkar V (2017) Unsupervised learning of disentangled representations from video. In: NeurIPS
20. Oh J, Guo X, Lee H, Lewis RL, Singh SP (2015) Action-conditional video prediction using deep networks in Atari games. In: NeurIPS
21. Denton E, Fergus R (2018) Stochastic video generation with a learned prior. In: Dy JG, Krause A (eds) ICML, series proceedings of machine learning research, vol 80
22. Shahabeddin Nabavi S, Rochan M, Wang Y (2018) Future semantic segmentation with convolutional LSTM. In: BMVC
23. Vora S, Mahjourian R, Pirk S, Angelova A (2018) Future segmentation using 3d structure. arXiv:1811.11358
24. Terwilliger A, Brazil G, Liu X (2019) Recurrent flow-guided semantic forecasting. In: WACV
25. Shi X, Chen Z, Wang H, Yeung D, Wong W, Woo W (2015) Convolutional LSTM network: a machine learning approach for precipitation nowcasting. In: NeurIPS
26. Wang Y, Long M, Wang J, Gao Z, Philip SY (2017) PredRNN: recurrent neural networks for predictive learning using spatiotemporal lstms. In: NeurIPS, pp 879–888
27. Wang Y, Wu H, Zhang J, Gao Z, Wang J, Yu PS, Long M (2021) PredRNN: a recurrent neural network for spatiotemporal predictive learning. arXiv:2103.09504
28. Yan J, Qin G, Zhao R, Liang Y, Xu Q (2019) IEEE Access. Mixpred: video prediction beyond optical flow 7:185654–185665. https://doi.org/10.1109/ACCESS.2019.2961383
29. Liu Z, Yeh RA, Tang X, Liu Y (2017) Video frame synthesis using deep voxel flow. In: Proceedings of IEEE international conference computer vision (CVPR), Oct 2017, pp 4463–4471
30. Wang Y, Jiang L, Yang M-H, Li L-J, Long M, Fei-Fei L (2019) Eidetic 3d LSTM: a model for video prediction and beyond. In: ICLR
31. Vondrick C, Pirsiavash H, Torralba A (2016) Generating videos with scene dynamics. In: NeurIPS
32. Tulyakov S, Liu M-Y, Yang X, Kautz J (2018) MoCoGAN: de-composing motion and content for video generation. In: CVPR

33. Aigner S, Körner M (2018) Futuregan: anticipating the future frames of video sequences using spatio-temporal 3d convolutions in progressively growing autoencoder GANs. arXiv:1810.01325
34. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, Courville A, Bengio Y (2014) Generative adversarial nets. In: Proceedings of advances neural information processing systems conference 2014, pp 2672–2680
35. Kwon Y-H, Park M-G (2019) Predicting future frames using retrospective cycle GAN. In: CVPR
36. Oprea S, Martinez-Gonzalez P, Garcia-Garcia A, Castro-Vargas JA, Orts-Escolano S, Garcia-Rodriguez J, Argyros A (2020) A review on deep learning techniques for video prediction. arXiv:2004.05214
37. Tulyakov S, Liu M-Y, Yang X, Kautz J (2018) MoCoGAN: decomposing motion and content for video generation. In: CVPR
38. Hochreiter S, Schmidhuber J (1997) Neural Comput. Long short-term memory 9(8):1735–1780
39. Cances J, Meghdadi V (2000) Annales Des Telecommun. Joint channel estimation and data demodulation algorithms for fast time varying band limited frequency selective Rayleigh fading channels: a comparison study 55(56):226–237
40. Schuldt C, Laptev I, Caputo B (2004) Recognizing human actions: a local SVM approach, vol 3. In: ICPR, pp 32–36
41. Srivastava N, Mansimov E, Salakhutdinov R (2015) Unsupervised learning of video representations using LSTMs. In: ICML
42. Horé A, Ziou D (2010) Image quality metrics: PSNR versus SSIM. In: 2010 20th International conference on pattern recognition, Istanbul, pp 2366–2369. https://doi.org/10.1109/ICPR.2010.579
43. Kingma D, Ba J (2015) Adam: a method for stochastic optimization. In: ICLR

System Using Profinet Communication for Improving a Laser Engraver

Milian Badea, Sorin-Aurel Moraru, and Vlad Ștefan Petre

Abstract This article presents a system created by the authors using Profinet communication for improving a laser engraver machine used in industrial processes for creating parts. Especially in the automotive industry, but also in many other manufacturing processes, a laser engraver is used to ensure the recognition and traceability of the parts within the production process. The system incorporates an operator panel for management, an easier way to define and apply engraving models, and a user permission system for better operability. The productivity is increased by changing the landmark involves two simple operations, changing the nest and the recipe. By introducing the Electronic Key system is eliminated unauthorized changes. Due to the RFID system and working with recipes is making impossible the incorrectly loading of the inscription program. The system allows modification of the laser program for each piece, and in the case of complex parts, data from the 2D code of the components received from another supplier to be found in the 2D code on the assembled part. Due to the multitude of messages and signals, an easy diagnosis of the machine is displayed on the operator panel, showing the status of the sensors on the machine, the status of the monitoring signals, and the error messages. A correct treatment of non-compliant parts by evaluating the signals and implementing the scrap box is making available.

Keywords System · Profinet communication · Laser engraver

M. Badea (✉) · S.-A. Moraru · V. Ș. Petre
Transilvania University of Brasov, B-dul Eroilor 29, 500036 Brasov, Romania
e-mail: milian.badea@unitbv.ro

S.-A. Moraru
e-mail: smoraru@unitbv.ro

V. Ș. Petre
e-mail: vlad.petre@unitbv.ro

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_18

1 Introduction

Laser engraving is the removal of material from the top surface down to a specified depth. Laser engraving is the practice of using lasers to engrave an object. The technique does not involve the use of inks, nor does it involve tool bits which contact the engraving surface and wear out [1].

Laser inscription is an innovation that is being broadly used as a part of metal and non-metal material preparing, which incredibly reduces the handling time and costs and improves the nature of work piece [2]. The main principle that a laser engraver works on is using a laser to inscript a piece of material of any kind and it is mostly used for modern assembling and generation applications. Laser engraving works by coordinating the yield of a powerful laser most regularly through optics [3].

In many branches of the nowadays industry the inscription process is used mostly in order to allow the identification of the final industrial products. The usage of this procedure is preferred over other methods, such as labeling or painting the products [4].

A laser engraving machine consists of three main parts: a laser, a controller, and a surface. Such a system can be built in many ways, the outcome being the same. Regardless the way it is build and managed, an engraving machine presents several advantages, e.g., being an economic, non-contact and a safe process, it can work on a range of depths and many types of materials, it is highly efficient and quality focused, it is a high-speed procedure and can be used in many domains for many applications [5].

The mechanism used by a simple engraving machine is very basic, thus there are many ways to improve the process done by it. There is needed a laser engraver machine controlled by a PLC controller and a predefined program uploaded for the specific model that should be engraved. Some enhancements could be added to this system, to ease the process overall. A PC is used for creating the model for inscription and uploading it to the machine, other devices are used to ensure an easy operation for the user such as operator panel, a solution to scan a model to get its code and level-based access permissions.

2 Improvements of Laser Engraver

In manufacturing processes, especially in the automotive industry, the inscription of the parts with both text and 1D or 2D is very important, on the one hand for their recognition on the production line and on the other hand for traceability in case of problem batches.

The construction and operation of the laser engraver machine before it was modernized was a classic and relatively simple one (see Fig. 1). A programmable automaton manages the sensors, the solenoid valves and the safety conditions.

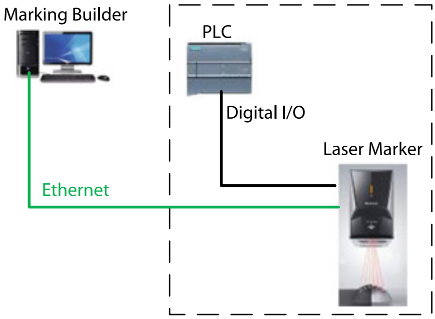


Fig. 1 Block diagram before modernization

The connection between the PLC and the Laser Marker was made from a hardware perspective, through the control Input/Output Terminal Block (16 pin), Contactor control terminal block (12 pin) and Control Input/Output MIL Connector (40 pin and 34 pin) interfaces.

Unlocking the Laser Marker was done with the safety relay in the emergency stop circuit and the closed-door confirmation limiter.

The control signals used were minimal for operation: *Trigger input*, *Trigger READY Output*, *Marking output* and *Marking complete output*.

The visualization of the operation mode of the Laser marker is done with the help of the Marking Monitor software, with its help the program is selected (previously transferred to the Laser Marker memory) when changing the reference.

The problems identified and that determined the modernization of the machine are the following:

- Due to the small number of interface signals some parts may be non-compliant, although the inscription process ends without error (for example when a 2D code is written and the Mark/2D Code Check signals are not checked OK Output, respectively, Mark/2D Code Check NOK Output).
- The person who selected the program when changing the reference could easily be wrong, especially with similar parts. Such a mistake could generate a very large number of non-compliant parts until it is identified, and the remedy requires a large consumption of money and time.
- Some more complex parts contain components received from another supplier, which in turn have inscribed a 2D code with the data of the respective manufacturer. There is a requirement for the end customer that the 2D code on the assembled part contain the data of all components. This could not be done because there is no scanner to read these codes or the possibility of transferring this data to the laser program.
- Because there is no scrap box, non-compliant parts could be placed, by mistake of the operator, on compliant parts.

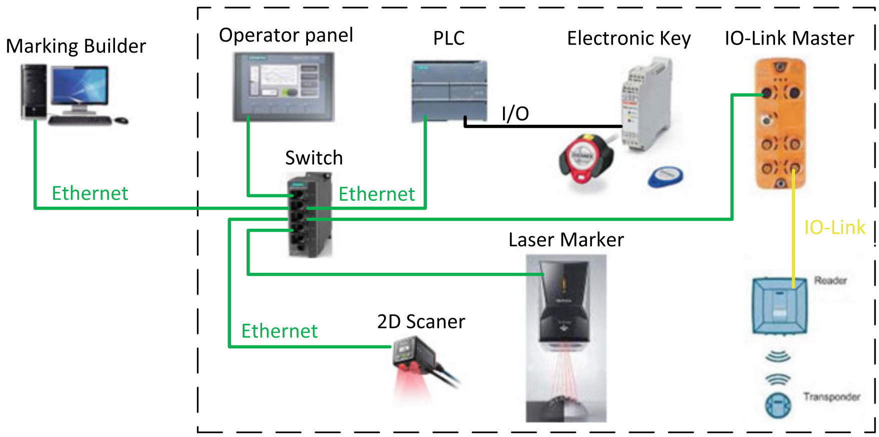


Fig. 2 Block diagram after modernization

In order to solve all these problems and in addition to make the machine more flexible for possible subsequent requirements, the equipment was modified as in Fig. 2.

3 System Components Function Description

3.1 Laser Marking with Profinet Communication

To ensure the Profinet connection between the Laser Marker and the Siemens PLC, the General Station Description (GSD) file is downloaded from the manufacturer's website and installed in the TIA Portal V14 programming environment library. The installation location is automatically chosen by the application, and to be inserted in the network it is found in the library on the path: *Other field devices/Profinet IO/Sensors/Keyence Corporation.*

In the *Device configuration/Device view* of the TIA Portal V14 programming environment you can see the allocation of I Address and Q Address. A total of 190 bytes are allocated in the input area, starting with IB200, and 154 bytes in the output area, starting with Q200.

The communication method is of the command-response type, so several commands cannot be sent simultaneously. Care must be taken to receive a response to an order, regardless of whether it is a confirmation or an error.

The main commands used in the program are:

- Q202.0—"Program Change Request" response I210.0—"Program Change Complete"
- Q200.0—"Start Marking Request" response I208.0—"Marking Complete"

- Q200.4—“2DC Read Request” response I205.5—“Mark Check/2DC Read OK Status” sau I205.6—“Mark Check/2DC Read NG Status”
- Q205.1—“Marked String Read Request” response I212.1—“Marked String Read Complete”
- Q205.2—“String Change Request” response I212.2—“String Change Complete”

The following commands were used to reset the confirmation and error bits:

- Q214.0—“Program Change Complete Bit Clear”
- Q212.0—“Marking Complete Bit Clear”
- Q216.1—“Marked String Read Complete Bit Clear”
- Q212.4—“2DC Read Complete Bit Clear”
- Q200.3—“Error Clear Request”

Because the Laser Marker allows reading the program written with the “Marked String Read Request” command, the first piece is printed with the unmodified laser program. Starting with the second part, after scanning the 2D code, the laser program changes. The program is read upon receipt of one of the signals “Mark Check/2DC Read OK Status” = 1 or “Mark Check/2DC Read NG Status” = 1 and written immediately after scanning a valid code. Successful writing in the Laser Marker of the modified program is signaled on the operator panel by the lamp in the vicinity of the text "Block sent”. This signal allows the launch of a new registration cycle.

3.2 2D Scanner with Profinet Communication

A 2D Scanner was introduced into the system so that 2D codes could be read and sent to the PLC as a string of up to 35 characters. Part of this string, according to the values set in the recipe, can be extracted and inserted in the laser program. The fields in the recipe that handle the string read by the 2D Scanner are:

- With/Without2DScaner (Bool)
- LenghtString2DScaner (Integer)
- NrByteStartRead (Integer)
- NrByteStartWrite (Integer)

The launch of the reading with Scanner is done by a photoelectric sensor that generates a digital signal when it detects the part in the scanner area, provided that the *With/Without2Dscaner* variable is ON. If the reading is done successfully in the Communication Buffer, the characters that make up the 2D code will be received, if the Error signal is not activated. The car will be locked until a valid code is received.

As in the case of Laser Marker, the General Station Description (GSD) file is downloaded from the manufacturer’s website and installed in the TIA Portal V14 programming environment library. The path of installation is the same: *Other field devices/Profinet IO/Sensors/Keyence Corporation.*

The way to allocate bytes in the input/output area of the PLC can also be seen in TIA Portal, in Device configuration/Device view. Out of the total of 128 Bytes allocated in the I Address area as read buffer "Read Data 128Byte_1", respectively, 128 Bytes allocated in the Q Address area as write buffer "User Data 128Byte_1" 35 characters are used. This number is determined by the maximum number of characters of the 2D code to be read.

Reading a code is initiated by activating output Q3.0 defined as Tag "StartScanKeyence" = 1. The appearance of the read trigger signal causes the scanner to try to read the code for 4 s.

If the reading is completed successfully, the scanner sets the I4.0 entry defined as Tag "CodeOK" = 1. This signal informs the PLC that a valid code has been transmitted, which is converted from a string to a length of 35; this string will extract the characters to be inserted in the laser program, according to the recipe already saved in the operator panel.

If the reading ends without success, the message "ERROR!" Is written in the string; and a signal is generated that locks the machine to a correct reading.

The signals used to evaluate the read operation are: I205.5—"Mark Check/2DC Read OK Status" and I205.6—"Mark Check/2DC Read NG Status".

3.3 RFID System

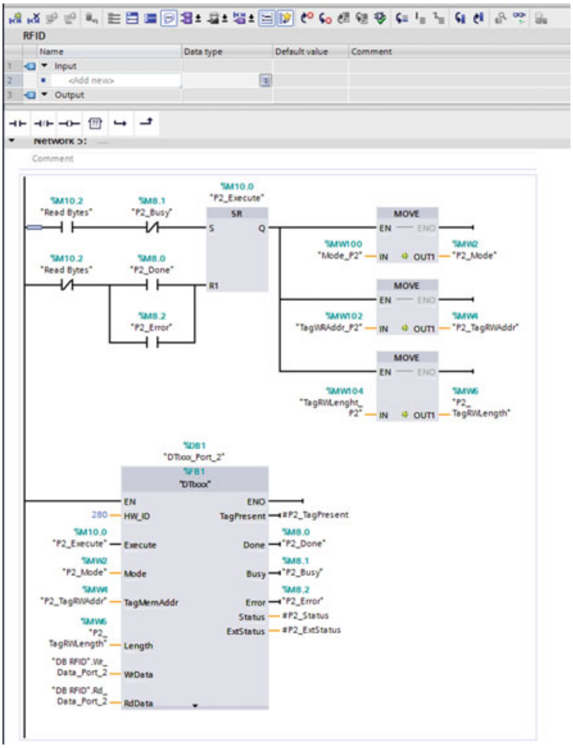
The Radio-frequency identification (RFID) system is composed of: IO-Link Master with Profinet interface, RFID read/write head, 13.56 MHz RFID tag.

The purpose of introducing this system is to exclude the possibility of incorrect inscription of a piece. For the correct inscription, several conditions must be met simultaneously:

- Positioning the inscription piece with respect to the laser at an exact distance (189 ± 21 mm);
- The piece should be positioned so that the laser beam is perpendicular to the surface;
- The laser program should be the right one.

To meet these requirements, for each piece a nest (support) was made on a 3-D print. An RFID Tag has been fixed on each nest, which is programmed with the landmark name. An RFID antenna has been mounted on the machine table, which will continuously read the TAG in its vicinity. The name of the piece inscribed on the RFID Tag will also be found in the production recipe, so that it is continuously checked if the name in the recipe and the one stored in the Tag are identical. If they are not identical, the machine will not start the cycle and an error message will be displayed.

Writing and reading TAGs is done via IO-Link Master via a Profinet communication via the FB1 function (DTIxxx) (see Fig. 3).



RFID

		Name	Data type	Default value	Comment
1		▾ Input			
2	▪	<Add new>			
3		▾ Output			

Fig. 3 Program diagram

The main parameters of the read/write DTIxxx function are:

Input Parameters:

- HW_ID—In the folder Hardware identifier you can see the Hardware identifier that the TIA Portal software has assigned to the DTIxxx device;
- Execute—activate the operating mode of the DTIxxx function block;
- Mode—operating mode of the DTIxxx function block
- = 4 read an area of the USER memory of the ID-TAG one time;
- = 5 write data to an area of the USER memory of the ID-TAG one time;
- TagMemAddr—start address in the USER memory of the ID-TAG to read or write data;
- Length—number of Bytes to read from or write to the USER memory of the ID-TAG;
- WrData—send buffer;
- RdData—receive buffer.

Output Parameters

- TagPresent—ID-TAG detected in the antenna field;

- Done—completed without error;
- Busy—operating mode in process;
- Error—operating mode abort with error;
- Status—status information or error code.

In the operating mode 4 the function block reads an area of the USER memory of the ID-TAG one time [6].

With the parameters TagMemAddr and Length select the source area in the USER memory of the ID-TAG. The destination area in the plc you assign at the parameter RdData.

When activating the operating mode 4, the function block latches the values of the parameters TagMemAddr and Length and initializes the data in the receive buffer first with 0 × 00. If an ID-TAG is present in the antenna field at this moment, the function block starts to transfer the data from the USER memory of the ID-TAG into the receive buffer.

The function block stores the read data in the receive buffer from the buffer start address onwards regardless of the source address in the USER memory of the ID-TAG.

If an error occurs, the function block stops reading and shows the error. If the DTIxxx device reports an error, the function block restarts the reading at the faulted position. After a certain number of failed attempts (3 by default) the function block shows the error.

When all data are read the function block shows the output parameter done = TRUE.

3.4 Electronic Key System

The electronic key system allows the achievement of access levels with different permissions.

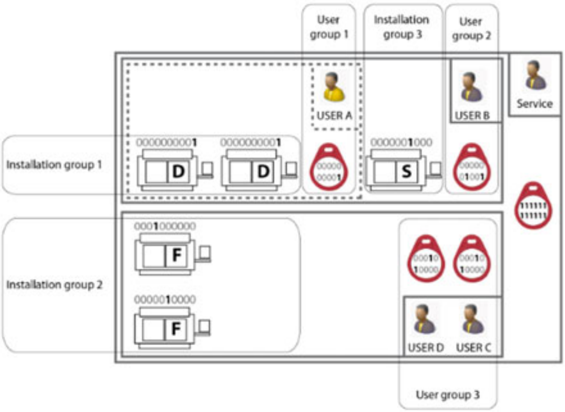
The system consists of a modular adapter in which the token is accessed to be read and an adapter interface that is mounted in the cabinet with devices and which through the parallel 4-bit interface transfers the access level.

The adaptation interface has 16 DIP switches with the following function:

- Bit0… Bit9—Encode the access code;
- Bit10… Bit13—Coding operating state;
- Bit14—It has no function;
- Bit15—Parity bit.

The access code has a length of 10 bits. The 10 bits for setting the code are available as a DIP switch on the adaptation interface or in the electronic key for programming in binary encoding. The access code results from the individual setting of the bits represented by the DIP switch in the interface and the individual setting of the bits

Fig. 4 Operating state 1 diagram



in the access code of the electronic key. A unique value generated by setting these bits with a value between 0 and 1023 is possible for the access code.

The system allows operation in 2 modes (operating state):

- Operating state 0—only an exact match of the bit pattern between the electronic key and the adaptation interface will allow access;
- Operating state 1—the matching within the bit pattern between the electronic key and the interface for adapting any bit will allow access.

Operating state 1 allows for greater flexibility by creating groups. The example of how to work in Operating state 1 is presented in Fig. 4.

Each token comes from the factory inscribed with a unique serial number (byte116 … byte 123). Chip programming involves:

- Writing an operating state (OS), an access level (AL) and an access code (AC) in bytes 110… bytes 113;
- Calculation of the checksum, using the values written in bytes 110… bytes 113 and serial number of the token;
- Writing the token with the values thus prepared.

Electronic key adapter with USB interface code EKS-A-IUX-G01-ST01 and Transponder Coding software were used to program the tokens. This is the cheapest, but more complicated programming possibility because the checksum (CRC—Cyclic Redundancy Check) must be calculated separately and the bytes are written in hexadecimal.

Because the checksum is calculated using the hexadecimal value of the control byte and those representing the serial number of the token, it will be different from token to token, even if the tokens are identical in operation (same operation state, access level and access code). It turns out that cloning a token will not work, each token must be programmed.

Two types of chips were used, obtaining three levels of access, as follows:

- No token—operator mode. In this mode, only reset buttons (error reset and part number reset) are active on the operator panel. The production recipe cannot be changed;
- Blue token—the regime assigned to the exchange manager. In this mode, the RECIPE button becomes active, with which a new recipe can be loaded. In this mode it is allowed only to load the recipe in the programmable machine and not to edit (modify) them. Remember that uploading a new recipe requires changing the nest;
- Red token—the regime assigned to the process engineer. In this regime it is allowed both to upload a new recipe and to modify it if necessary. RFID chip programming is also allowed.

3.5 Operator Panel for Setting and Viewing Parameters

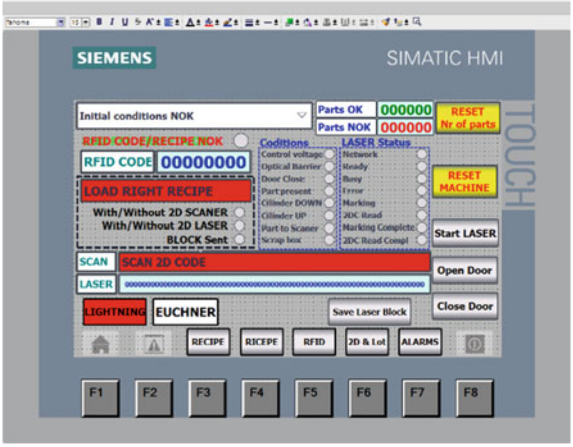
The operator panel allows the visualization of various messages and states but also the realization of production recipes that are essential in the operation of the machine.

The status of the sensors on the machine is visualized in the conditions area by lamps: gray—low status, green—high status. Similar for signals in the LASER status area with the specification that all these signals are received from the laser recorder on communication (see Fig. 5).

The laser program and the string read with the scanner are displayed from which certain characters are extracted and then inserted into the laser program.

The recipe structure is:

- Program (Integer)—no laser program;
- LenghtStringProgLaser (Integer)—Laser program length;


Initial conditions NOK

Parts OK 000000

Parts NOK 000000

RFID CODE 00000000

Fig. 5 Operator panel for setting and viewing parameters

- With/Without2DLaser (Bool)—With/Without verification 2D Code after registration;
- With/Without2DScaner (Bool)—With/Without reading 2D code with scanner
  - LenghtString2DScaner (Integer);
  - NrByteStartRead (Integer);
  - NrByteStartWrite (Integer);
- With/WithoutData (Bool)—With/No read/write date
  - NoByteStartWriteData (Integer);
- With/WithoutCounter (Bool)—With/Without reading/writing counter
  - NrByteStartWriteCounter (Integer).

Depending on the settings in the recipe, the machine can work with or without changing the laser program. In both cases, the selection of the laser program is done automatically when the recipe is loaded. It is also possible to check the 2D code after registration.

Before starting the production, the recipe is selected and the nest is installed according to the landmark. If the RFID code matches the name in the recipe, the RFID Code/Recipe OK essay can begin.

4 Operation Without Modification of the Laser Program

Disable the following recipe fields:

- With/Without2Dscaner = 0
- With/WithoutData = 0
- With/WithoutCounter = 0

The start of the inscription cycle starts automatically when the piece is placed in the nest and the light barrier is not interrupted. After closing the door, the cycle goes like this:

- Select laser program “Program Change Request AUTO” = 1;
- Confirmation of the program change “Program Change Complete” = 1 determines the start of the registration “Start Marking Request AUTO” = 1;
- Confirmation “Marking Complete” = 1 determines the verification of the 2D code written “2DC Read Request AUTO” = 1;
- The signals “Mark Check/2DC Read OK Status” = 1 or “Mark Check/2DC Read NG Status” = 1 represent the end of the cycle and the door opening is commanded.

5 Operation with Modification of the Laser Program

Disable the following recipe fields:

- With/Without2Dscaner = 1
- With/WithoutData = 1
- With/WithoutCounter = 1

The 2D code is scanned; the characters that you want to insert in the laser program are automatically extracted, according to the values set in the recipe.

The start of the inscription cycle starts automatically when the piece is placed in the nest and the light barrier is not interrupted and takes place as above.

The signals “Mark Check/2DC Read OK Status” = 1 or “Mark Check/2DC Read NG Status” = 1 also represent in this situation the end of the cycle and the door opening is commanded.

When one of the two signals appears, the laser program is triggered (2D Code from Block1 and Data and Counter from Block2).

Scanning the 2D code, modifying the laser program and successfully transferring it is a condition for starting the next registration cycle.

6 Conclusions

The modernization was imposed by both aspects related to productivity and elimination of errors but also by the customer and solved the following aspects:

Increasing productivity by changing the landmark involves two simple operations, changing the nest and the recipe. No other settings or adjustments are required, all data required for production remain saved in the operator panel (HMI), Laser Marker and Scanner.

Elimination of unauthorized changes by introducing the electronic key system. By achieving access levels with different permissions, only the process engineer has access and permission to modify recipes and program RFID tokens.

Impossibility of incorrectly loading the inscription program due to the RFID system and working with recipes. The name of the recipe and the code stored in the RFID Tag must be identical for the machine to allow automatic cycle start.

Possibility to modify the laser program for each piece. In this way there is the possibility that in the case of complex parts, data from the 2D code of the components received from another supplier (manufacturer code, batch, date of manufacture), to be found in the 2D code on the assembled part. In this way, the final beneficiary has all the necessary data by reading a single 2D code.

An easy diagnosis of the machine due to the multitude of messages and signals displayed on the operator panel. You can see the status of the sensors on the machine, the status of the monitoring signals (digital input for the PLC) and control (digital output for the PLC) of the Laser Marker and the error messages.

Correct treatment of non-compliant parts by evaluating the “Mark Check/2DC Read OK Status” and “Mark Check/2DC Read NG Status” signals and implementing the scrap box. This is because the reset of the “Mark Check/2DC Read NG Status” signal (which locks the machine for the next cycle) is done only by the photoelectric sensor of the waste box, so the operator is obliged to put the non-compliant parts in this box.

References

1. Patel S, Patel SB, Patel AB (2015) A review on laser engraving process. IJSRD—Int J Sci Res Dev ISSN (online) 2321-0613
2. Kumar J (2016) Evaluation of mechanical properties of natural fiber of reinforced composit. Int J Comput Sci Eng Res 4(5):77–86
3. Kumar J, Siva Sai Tarun A, Gowtham M, Yashwanth M (2017) Design and fabrication of portable laser cutting and engraving machine. Int J Eng Technol 7(1–1):570
4. Lazov L, Deneva H, Narica P (2015) Laser marking methods, environment technology resources. In: Proceedings of the international scientific and practical conference, vol 1, p 108
5. Markov LL, Lebedeva LI, Kanatnikov NV (2015) Results of research on causes of the defects of laser marking articles. In: IOP conference series materials science and engineering, vol 91, no 1
6. IFM Electronic Gmbh, Description S7-1200 and S7-1500 function block DTIxxx, version 1.2 (2019)
7. Keyence (2016), Marking Builder 3 user manual
8. Keyence (2016), Laser marker PROFINET communication user interface
9. Siemens AG (2016) STEP 7 professional V14 system manual

Verification and Validation for a Project Information Model Based on a Blockchain

Will Serrano and Jeremy Barnett

Abstract Agile project management based on minimum viable products has some benefits against the traditional waterfall method. Agile supports an early return of investment that supports circular reinvesting and makes the product more adaptable to variable social-economical environments. However, agile also presents some intrinsic issues due to its iterative approach. Project information requires an efficient record of the requirements, aims, governance not only for the investors, owners or users but also to keep evidence in future health and safety and other statutory compliance-related issues. In order to address the agile project management issues and address new safety regulations, this paper proposes a project information model (PIM) based on a distributed ledger technology (DLT) with a ranked procedure for the verification and validation (V&V) of data. Each V&V phase inserts a process of authenticity, data abstraction and analytics that adds value to the information founded on artificial intelligence (AI) and natural language processing (NLP). The underlying DLT consists of smart contracts embedded on a private Ethereum blockchain. This approach supports a decentralised approach in which every project stakeholder owns, manages and stores the data. The presented model is validated in a real scenario: University College London—Real Estate—Pearl Project.

Keywords Smart contracts · Blockchain · Information model · Real estate · Artificial intelligence

1 Introduction

Failure of large construction projects is caused by various factors, including delays or changes in specification, lack of a single source of truth across the different project

W. Serrano (✉) · J. Barnett
The Bartlett, University College London, London, UK
e-mail: W.Serrano@ucl.ac.uk

J. Barnett
e-mail: Jeremy.Barnett@ucl.ac.uk

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_19

stages, value engineering and cost overruns. Traditional waterfall project management has proved inadequate in complex construction projects, where more agile and lean approaches have already demonstrated success. Minimum viable products that deliver an early return of investment are becoming investors' preference as they are more adaptable to a variable socio-economic environment. Hybrid management conceptual models unite improved communications, flexibility and the reduction of design changes by combining the 'waterfall', 'lean' and 'agile' approaches. Hybrid builds upon total quality management (TQM) and just in time (JIT) principles [1]. The agile option of 'fast projects' based on a gradual, iterative and progressive delivery has the inherent risk that the project may always finish in the next iteration. Agile requires the management and supervision of quality in terms of requirements, aims, governance and health and safety.

To support a successful agile delivery, project information models (PIMs) are established within the design and construction stages of a project. PIMs assures that the data, such as requirements or meeting minutes, are validated at every project stage. This validation confirms its accuracy, compliance with standards and final completeness. This information is normally in the Employer's Information Requirements (EIRs) and the common data environment (CDE) as the single source of truth where the entire project team shares responsibility. The Hackitt review has recognised the importance of a data-driven strategy supported by a PIM in the Grenfell Tower disaster. The draft building safety bill [2] defines the government's proposals to reform the regulatory system for buildings. In addition, there must be a safety case report as a live document that requires continual review with mandatory reporting requirements. These wide-ranging recommendations are likely to become legal requirements in due course. For example, although the current definition of higher-risk buildings is currently limited to multi-occupied residential buildings of over or six storeys, these regulations could potentially apply to office blocks. Owners and property managers of all relevant real estate need to take steps to introduce a system capable of delivering compliance to protect not only the inhabitants but also their employees.

In order to address the agile project management issues and address new safety regulations, this paper proposes a PIM based on a distributed ledger technology (DLT) with a ranked procedure for the verification and validation (V&V) of data. Each V&V phase stage inserts a process of authenticity, data abstraction and analytics that adds value to the information founded on artificial intelligence (AI) and natural language processing (NLP). Data are initially introduced by different project users and stakeholders via a Web page and then inserted into the PIM. The underlying DLT consists of smart contracts embedded on a private Ethereum blockchain. This approach supports a decentralised approach in which each project stakeholder owns, manages and stores the distributed ledger data, therefore removing the need for a centralised or information management system or assessor. The practical application of the presented PIM includes three phases of verifications:

- Bronze verification: insertion of the data into the smart contract developed within a private Ethereum blockchain;

- Silver verification: analysis of the inserted data in the bronze validation extracting its relevant topics via AI and NLP;
- Gold verification: evaluation of the sentiment and content classification of the text stored in the silver validation via AI and NLP.

The proposed solution collects information from the different project stakeholders via a Web page and stores it within the PIM via a private Ethereum blockchain. The verification and validation of the PIM have been applied to a real scenario with static data: University College London, Real Estate Pearl Project. First, Sect. 2 describes the research background of verification and validation models. Then, Sect. 3 presents the verification and validation models of the PIM, whereas Sect. 4 presents its practical implementation. Finally, Sect. 5 shares the research conclusions.

2 Research Background

There are numerous V&V methods and statistical techniques although it is unpractical to apply all of them. V&V techniques and approaches can be classified based on different characteristics and their applicability to the different models and simulations. Effective and efficient V&V methods consist of these precise features: access to data from real systems, suitability for a virtual simulation, type of requirements and type of study and finally access to the source code [3]. Unfortunately, the concepts of V&V are commonplace, and both terms are considered interchangeable. A definer is embedded at the beginning of the word that distinctly indicates its context based on the V&V and the systems engineering ‘V’ model [4]. Agent-based simulations are cost-effective methods for V&V assessments although they present challenges as well. Whilst there are numerous model standards for design, verification, validation and presentation, the different theoretical strategies and the relation between models against reality often remain undefined [5].

2.1 Software

V&V has a key role in the life cycle of software development, particularly within the safety–critical sector. Cyber-physical systems (CPSs) are composed of physical and software subsystems. Numerous tools are available based on simulations that enable the design of CPS and the V&V process although their integration poses a great interoperability challenge. A solution is an open-source software environment for modelling and simulation based on an open standard language and sandbox [6]. A competition on software verification requires a thorough comparative assessment of every autonomous software verifier to guarantee effectiveness and efficiency [7].

2.2 Artificial Intelligence

A controller based on a neural network controls actions in an autonomous robot based on the analyses of LIDAR images. This method is verified from a safety perspective via a finite-state abstraction [8]. The manual software graphics verification of display dashboards with multiple static and dynamic objects is a time-consuming task that generates additional errors. A method that detects graphics symbols from complex synthetic backgrounds verifies graphics symbols and alphanumeric objects following software requirements based on deep learning [9]. Developers and users of an AI and machine learning system are provided with a multisource AI scorecard table for a standard V&V checklist [10]. V&V approaches that assess the navigation algorithms of autonomous surface ships are based on simulations with limited scenarios that are developed manually. A testing approach combines the training of neural networks based on reinforcement learning to choose challenging scenarios for the autonomous system [11].

2.3 Safety Critical

There is a growing demand for new functionality in safety–critical systems based on technology. This fast incorporation of commercial software and hardware brings additional risks with the increment of life-threatening vulnerabilities. A framework for the development of safety–critical systems consists of traditional methods and includes a development process that documents the requirements of the different systems [12]. The design and regulation of fire performance models in buildings and transport infrastructure have generated a growing development and application of fire simulation and models. The V&V for computational fluid dynamics models for fire safety models cover the estimates of errors within a design based on performance and different fire scenarios [13]. The formal V&V of industrial safety–critical applications such as signalling requires the definition of the verification rules based on the formulation of a large number of mathematical assumptions. A genetic programming and mutation-based validation technique support the development of verification rules to establish the validity and completeness of these assumptions [14].

2.4 Systems Engineering

The design of system of Systems poses challenges due to the current and independent application of (1) large brute-force tests that are very limited in the conditions range they can simulate and (2) simplistic models for formal V&V that do not reflect reality. A simulation model framework of system of systems for V&V integrates formal analytic and simulation verification methods [15]. The development and operation of virtualised control in Industry 4.0 systems can be used as a tool for the V&V system life cycle or the creation of a comprehensive digital model of the system. However, in practice, a digital twin built entirely from a digital technology often does not operate well due to the lack of a formal description or incomplete synchronisation between the continuous-time nature in the real system and the discrete behaviour of the computer model [16].

2.5 Internet of Things

Introducing the Internet of Things (IoT) in Industry 4.0 may originate novel accidents and hazards due to the enablement of remote operations and the operation of low power and low bandwidth devices. The expansion of IoT environments in cloud computing also requires scalable V&V techniques for large IoT safety–critical systems. Software engineering for the IoT needs a software development life cycle and support safety and quality control with assurance actions on environments that must contain privacy and safety at all network, processing and storage levels [17].

2.6 Autonomous Cars

The process of V&V of automated vehicles requires a safe operation in random complex and infinite-dimensional domains. An analysis of the critically of a system maps an infinite-dimensional domain onto a finite and manageable set of artefacts [18]. Image-assisted driving technology is part of collision avoidance systems. A 3D engine simulator uses specific data sets to test and verify various classic algorithms of vision-based recognition, identification and ranging [19].

2.7 Blockchain and Smart Contracts

The migration from a centralised information system to a blockchain information system requires a method for users to verify it. An efficient pre-verification data model for electronic documents in blockchain trading is based on an integrated verification method [20]. Furthermore, the V&V of smart contracts presents issues that consist of the shared understandings and intentions of the parties, the software code and a natural language contract [21].

2.8 Robots

The consequences of robotic failures in citizens, businesses, insurance and certification companies require manufacturers and software developers to confirm that the most critical sections of the software code are reliable and error free with a formal V&V certification [22]. The V&V in robotics must consider the coexistence of different models and the completeness of each other, including the telecommunication and middleware layers. In addition, V&V of AI in robotics must also integrate human presence and interaction as part of the process. The standardisation of COTS components and interfaces within software intensive systems whilst still complying with international standards imposes large requirements within the V&V process and highlights the challenges of robotics and the new space age [23].

2.9 Images

Photos are used as evident material in news reporting; therefore, manipulated or tampered pictures generate misinformation which is a lack of trust in journalism. The image verification industry must balance forensic automation and human experience to protect the audience from inaccurate information propagation [24].

3 Verification and Validation Model

The project information model is modelled as an N-dimensional universe of Z data elements in which every item is different from the others. The universe from which the PIM is generated is defined as a relation V formed of a set of Z N-tuples, $V = \{u_1, u_{2,} \ldots u_Z\}$, where $u_0 = (p_{01}, p_{02} \ldots p_{0N})$ is data item, o and p_0 are the N different data attribute values for $i = 1, 2, \ldots, Z$. The crucial idea within this proposed method is that data are defined as $D_{\mathrm{t}}(m(t), s)$ in which:

- $m(t)$ is a variable M-dimension vector with $1 < M < N$ where items are included or removed based on data analytics;
- t is the validation and verification phase where t where $t > 0$;
- s is the value of the data D_{t} at time t.

The proposed PIM method applies a ranked algorithm where data stakeholders validate and verify data. This process adds quality as it authenticates data or provides additional data analytics services. The method of validation and verification, VV_{AB}, is defined as:

- Row stakeholders $(1, \ldots, a, \ldots A)$ provide the data validation service: this A method approves the data stored in the smart contract as authentic;

- Column stakeholders (*1*, …, *b*, … *B*) provide the data verification service: this *B* method includes data analytics that adds value to the information.

Data value *s* of $D_t(n(t), s)$ at a time or phase *t* is defined as:

$$s = \sum_{b=1}^{B} b^2 * \sum_{a=1}^{A} a \qquad (1)$$

Each row *a* performs as a data checker that approves the introduced data into the marketplace by a stakeholder. On the other hand, each column *b* analysis the data in terms of filtering, aggregation and refining that satisfies the different information needs from external or internal clients and customers. In another word, the more rows A the more authentic the data are and the more columns *B*, the more valuable (Fig. 1). The practical application of the proposed V&V method consists of a service model based on bronze, silver and gold verification:

- Bronze verification certifies the data are genuine and authentic and inserts it into the private ethereum blockchain via a smart contract;
- Silver verification introduces additional data analysis. This layer extracts the main topics via natural language processing (NLP) and artificial intelligence (AI) algorithms from the bronze verification;
- Gold verification purpose is to evaluate the sentiment and the content classification of text stored in the silver validation via AI and NLP.

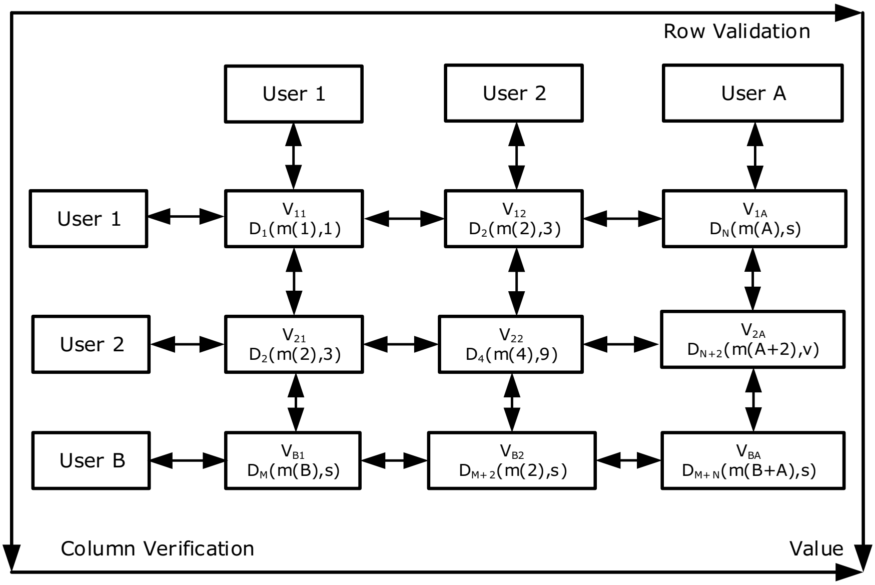


Fig. 1 Data marketplace model

4 Experimental Results

4.1 Project

The proposed V&V for a project information model has been validated in University College London (UCL), Real Estates PEARL Project. Person Environment Activity Research Laboratory (PEARL) is the UCL's first in-use building with a net-zero carbon balance. PEARL was designed as an urban prototype laboratory to generate large size environments that test how people use infrastructure and cities. The 'DigitalDisruption' consortium at UCL was established to pilot new technologies in live situations including the testing of PIM platforms to capture critical information about the construction project. PEARL has been selected as a laboratory for safety, creating an ideal opportunity to model fire safety and other statutory data via a stage gateway method for project management.

4.2 Technology

The PIM Web page acquires information from the project stakeholders via a Web page where information is transmitted with HTTPS protocols and information stored in a SQL database (Fig. 2). The proposed V&V model stores the retrieved information in the blockchain. The V&V method is implemented using Geth Ethereum and the smart contract using solidity. The backend server runs on Linux with Java maven where the embedded blockchain and smart contracts are managed by the web3j library.

The NLP is outsourced to the Google Cloud Services API based on three services (Table 1):

1. Entity analysis provides a salience score for known concepts such as a person, an organisation, or location entities. The salience score provides information

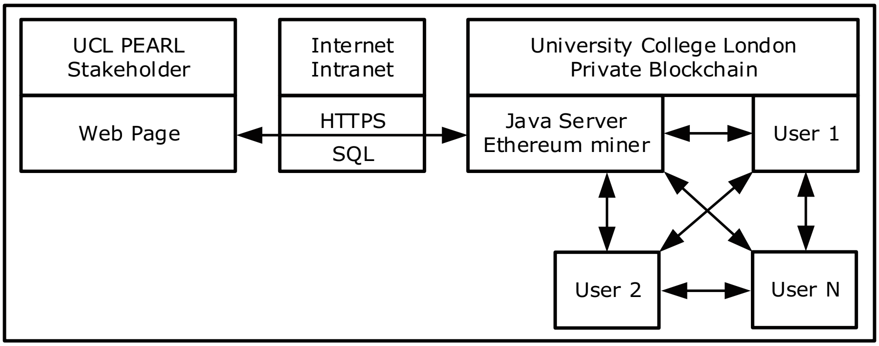


Fig. 2 Project information model architecture

Table 1 NLP Google Cloud Services

Text	'A fire broke out in the 24-floor Grenfell Tower on the June 14th, 2017. 72 deaths were caused by the fire; this number includes two victims who died in hospital at a later day. This fire is considered the worst UK residential fire since the Second World War and deadliest structural fire in the United Kingdom since the 1988 Piper Alpha disaster'
Salience	Fire: 0.58, Victims: 0.12, Grenfell Tower: 0.09, Deaths: 0.05
Score and magnitude	−0.5 and 1.7
Category	Sensitive subjects: 72%
Text	'Grenfell Tower was placed within a council housing complex in North Kensington; specifically, it was part of the Lancaster West Estate. Clifford Wearden and Associates designed the 24-floor tower block in 1967 following the Brutalist style of the generation. Its construction was approved by the Kensington and Chelsea London Borough Council in 1970'
Salience	Part: 0.25, Tower Blocl: 0.24, Lancaster West Estate: 0.20
Score and magnitude	0.0 and 0.0
Category	Arts and entertainment/visual art and design/architecture: 70% Real estate: 59%
Text	'A new regulatory framework is proposed by the Hackitt review that recommends the encouragement of genuine system transformation for the creation of a simpler and more effective process to drive building safety, provision of stronger oversight of duty holders based on incentives for the right behaviours'
Salience	Review: 0.26, Hackitt: 0.18, System transformation: 0.15
Score and magnitude	0.3 and 0.3
Category	Law and government/legal: 50%

about the importance of the entity within the entire document text from 0.0 as less salient to 1.0 as highly salient.

2. Sentiment analysis determines the overall positive or negative attitude expressed within a document. Sentiment is composed by:

- Score (S): the normalised value of the sentiment ranges between -1.0 for negative sentiment and +1.0 for positive sentiment. Score corresponds to the overall emotional learning;
- Magnitude (M): the unnormalised value between 0.0 and $+\infty$ represents the overall strength of the positive or negative emotion. Magnitude is generally proportional to the length of the document.

3. Category analysis clusters the document into a list of content categories.

4.3 Verification and Validation

The purpose of the experimental results is the confirmation of the V&V proof of concept for the proposed PIM. Every time there is either a validation or verification phase as a consequence of an increment of *t*, two smart contract transactions are generated:

- Data Analysis (DA): generated by the AI and NLP algorithms that perform data analytics;
- Data Value (DV): represents the value s of the V&V phase.

The proposed V&V PIM has analysed and stored meeting minutes at various stage gateways. Table 2 shows the different values for the V&V PIM from NLP Google Cloud Services.

Table 3 defines the smart contract variables for the V&V process.

Table 2 V&V PIM NLP Google Cloud Services

Gateway	Gate 2—Stage 1—Phase 1
Salience	Design responsibility matrix: 0.065, Project team: 0.030 Project: 0.028, Project procedures document: 0.023
Score and magnitude	0.0 and 4.2
Category	Business and industrial: 50% Construction and maintenance: 50%
Gateway	Gate 2—Stage 2—Phase 2
Salience	Stages: 0.072, Option: 0.049, UCL Centre for transport studies: 0.035, Stage: 0.033, Project: 0.031, Principal designer: 0.027
Score and magnitude	0.0 and 9.4
Category	Real estate: 76% Business and industrial: 62% Construction and maintenance: 62%
Gateway	Gate 2—Stage 2—Phase 3
Salience	Option: 0.049, Stage: 0.033, Project: 0.031, UCL Centre for transport studies: 0.028, Principal designer: 0.028
Score and Magnitude	0.0 and 9.9
Category	Real estate: 76% Business and industrial: 62% Construction and maintenance: 62%
Gateway	Gate 3—Stage 3—Phase 1
Salience	Design update architectural: 0.1286, Signage: 0.0413, Designs: 0.0312, Stage: 0.0285, Risk management register: 0.0245
Score and magnitude	0.0 and 16.4
Category	Business and industrial: 53% Business services: 53% Construction and maintenance: 50%
Gateway	Gate 4—Stage 4—Phase 1
Salience	Government guidelines: 0.025, Extension: 0.0219, Stairs: 0.0213, Fire rating: 0.0213, Health and Safety: 0.0176, UCL: 0.0174
Score and magnitude	0.0 and 17.3
Category	Business and industrial: 50% Construction and maintenance: 50%

Table 3 Smart contract variables

Variable	Value
Account address	0 × a35b5e29e84161c9aa75d519dd8f947f7e8e9eea
Contract address	0 × 19de1e2653a9bcf8ae305c71e7b75c484e9e7a67
Gas limit	22,000,000,000
Gas price	21,000

4.4 Row Validation

The various row validations phases approve the data extracted from the different project gateways and confirm its authenticity. Table 4 represents the average figures for the five different simulations with experimental for the data analysis (DA) and data value (DV) with their respective transaction fees, gas price and mining time.

The results from the row validation confirm the general blockchain equation where the transaction fee (GWEI) equals the multiplication of the gas limit by the gas price (Table 4). Data value (DV) has a lower transaction fee, or it is less expensive to mine, with a more reduced time than the data analysis (DA). This is due to DA inserting a larger block structure into the blockchain, specifically, a single array of double type numbers instead of a single integer type number, respectively (Fig. 3). In addition, the transaction fees and time figures do not follow a linear correlation to the volume of data stored within the blockchain (Fig. 3).

Table 4 Row validation—blockchain and smart contracts

Validation stage	Data input	Gas price	Transaction fee (GWEI)	Mining time	V&V value *v*
Initialisation	N/A	2.58E+05	5.69E−03	7.96E−04	0
1-DA	8726	3.93E+06	8.64E−02	3.77E−03	1
1-DV	1	4.20E+04	9.24E−04	9.28E−04	
2-DA	8726	2.91E+05	6.40E−03	2.84E−03	2
2-DV	1	2.70E+04	5.94E−04	1.07E−03	
3-DA	8726	4.92E+05	1.08E−02	4.83E−03	3
3-DV	1	2.70E+04	5.94E−04	6.25E−04	

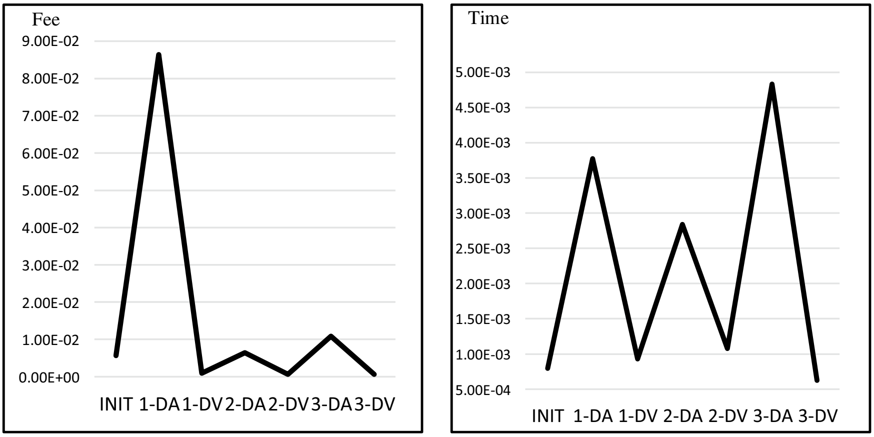


Fig. 3 Row validation—transaction fee and mining time

4.5 Column Verification

The different column validations phases apply data analytics to add value to the information based on artificial intelligence (AI) and natural language processing (NLP). The bronze verification introduces the extracted project gateway minutes into smart contracts confirming its authenticity. The silver verification extracts the salience of the bronze verification, whereas the gold verification stores the score, magnitude and category. Table 5 represents the average figures for the five different simulations with experimental results for the data analysis (DA) and data value (DV) with their respective transaction fees, gas price and mining time.

The column verification also supports the transaction fee (GWEI) equation with uniform results as row validation (Table 5). The mining time of the blocks and their associated transaction fees rely more on the block structure instead of the volume of information stored within the block itself (Fig. 4).

Table 5 Column verification—blockchain and smart contracts

Validation stage	Data input	Gas price	Transaction fee (GWEI)	Mining time	V&V value *v*
Initialisation	N/A	2.58E+05	5.69E−03	1.07E−03	0
1-DA	8726	3.93E+06	8.64E−02	4.37E−03	1
1-DV	1	4.20E+04	9.24E−04	9.09E−04	
2-DA	7790	8.91E+05	2.39E−02	5.05E−03	4
2-DV	1	2.70E+04	5.94E−04	6.00E−04	
3-DA	75	4.93E+05	1.08E−02	3.85E−03	9
3-DV	1	2.70E+04	5.94E−04	7.03E−04	

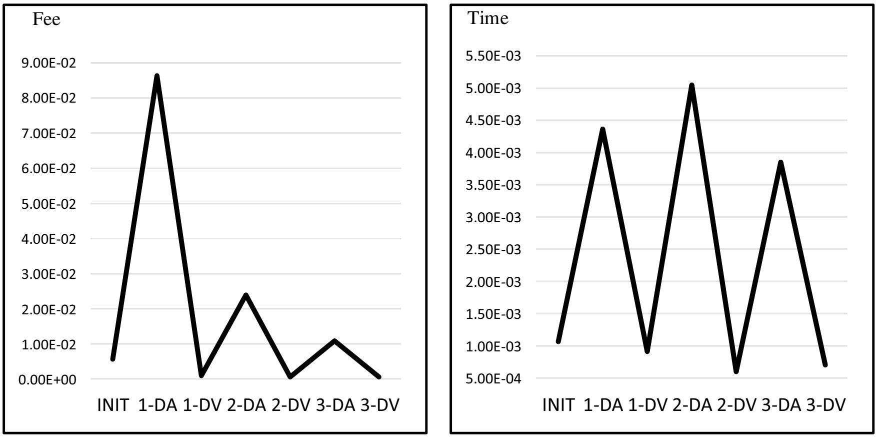


Fig. 4 Column verification—transaction fee and mining time

5 Conclusions

This paper has presented a verification and validation algorithm for a project information model (PIM) based on a distributed ledger technology (DLT). The proposed algorithm is founded on a ranked procedure for the verification and validation (V&V) of data where each V&V phase inserts a process of authenticity, data abstraction, and analytics that adds value to the information based on artificial intelligence (AI) and natural language processing (NLP). The proposed model has been validated in a real application with live data: University College London Real state—PEARL Project. The results obtained from several experiments confirm that solidity smart contracts based on a private Ethereum blockchain successfully add value to the information in a decentralised network. The blockchain presents a linear correlation between the gas limit, gas price and transaction fee. The mining time and the transaction fee rely more on the block structure instead of the volume of information stored within the block itself.

Author Contributions
Will Serrano is the writer of the paper. His contribution covers the literature review, verification and validation model, artificial intelligence, blockchain implementation and experimental results. On the other hand, Jeremy Barnet included the law-related elements, the application of a PIM model into a V&V process and the project PEARL with related information and data.

Acknowledgements Both authors of this paper would like to thank UCL Estates and Greystar for funding the publication of this research.

References

1. Oakland J (2014) Total quality management and operational excellence. 1–555
2. https://www.gov.uk/government/publications/draft-building-safety-bill
3. Roungas B, Meijer S, Verbraeck A (2018) A framework for optimizing simulation model validation & verification. Int J Adv Syst Measure 11(1,2):137–152
4. Ryan M, Wheatcraft L (2017) On the use of the terms verification and validation. In: International council on systems engineering international symposium, vol 27, no 1, pp 1277–1290
5. Grabner C (2018) How to relate models to reality? An epistemo-logical framework for the validation and verification of computational models. J Artif Soc Soc Simul 21(3, 8):1–26
6. Sinisi S, Alimguzhin V, Mancini T, Tronci E (2021) Reconciling interoperability with efficient verification and validation within open source simulation environments. Simul Model Pract Theory 102277
7. Beyer D (2017) Software verification with validation of results. In: International conference on tools and algorithms for the construction and analysis of systems, pp 331–349
8. Sun X, Khedr H, Shoukry Y (2019) Formal verification of neural network controlled autonomous systems. In: International conference on hybrid systems: computation and control, pp 147–156.

9. Pal D, Alladi A, Pothireddy Y, Koilpillai G (2020) Cockpit display graphics symbol detection for software verification using deep learning. In: International conference on data science and engineering, pp 1–5
10. Blasch E, Sung J, Nguyen T (2020) Multisource AI scorecard table for system evaluation. In: Association for the advancement of artificial intelligence artificial intelligence in government and public sector, pp 1–8
11. Porres I, Azimi S, Lafond S, Lilius J, Salokannel J, Salokorpi M. On the verification and validation of AI navigation algorithms. To be published
12. Kumar N, Lawford M, Maibaum T, Wassyng A (2021) A formal approach to rigorous development of critical systems. J Softw: Evol Process 1–27
13. Hees P (2013) Validation and verification of fire models for fire safety engineering. Procedia Eng 62:154–168
14. Laibinis L, Iliasov A, Romanovsky A (2021) Mutation testing for rule-based verification of railway signaling data. IEEE Trans Reliab 1–16
15. Zeigler B, Nutaro J (2016) Towards a framework for more robust validation and verification of simulation models for systems of systems. J Defense Model Simul: Appl Methodol Technol 13(1):3–16
16. Semenkov K, Promyslov V, Poletykin A (2020) Validation of control systems with heterogeneous digital models and virtualization technologies. In: Lecture notes in informatics, pp 299–309
17. Kotti J (2021) Software engineering for IoT with safety aspects. In: Safety in extreme environments, pp 1–5
18. Neurohr C, Westhofen L, Butz M, Bollmann MH, Eberle U, Galbas R (2021) Criticality analysis for the verification and validation of automated vehicles. IEEE Access 9:18016–18041
19. Du L, Lyu T, Zhu H, Wang X (2021) Validation of Vehicle detection and distance measurement method using virtual vehicle approach. In: International conference on graphics and image processing, vol 1172005–1, pp 1–10
20. Oh S, Cho S, Han S, Gim G (2019) A study on the pre-verification of data and the implementation of platform in electronic trade using blockchain. In: International conference on software engineering, artificial intelligence, networking and parallel/distributed computing, pp 320–330
21. Magazzeni D, McBurney P, Nash W (2017) Validation and verification of smart contracts: a research agenda. Computer 50(9):50–57
22. Ingrand F (2019) Recent trends in formal validation and verification of autonomous robots software. In: International conference on robotic computing, pp 321–328
23. Gomes C, Basso T, Mattiello F, Moraes R (2020) Impacts of the space technology evolution in the V&V of embedded software-intensive systems. In: International conference on computational science and computational intelligence, pp 1–7
24. Katsaounidou A, Gardikiotis A, Tsipas N, Dimoulas C (2020) News authentication and tampered images: evaluating the photo-truth impact through image verification algorithms. Heliyon 6(2):1–22

Automatic Synthesis of Cognitive Model for Revealing Economic Sectors' Needs in Digital Technologies

Alexander Raikov, Alexei Ermakov, Alexander Merkulov, and Sergey Panfilov

Abstract The paper addresses the automation of cognitive modelling for decision-making support in revealing economic sectors needs in digital technologies. It requires to take into consideration many factors, some of which have non-formalizable character. Some aspects do not have retrospective statistic history and are latent. Cognitive modelling is one of the artificial intelligence (AI) methods for describing such situations. It considers factors of enriching AI models by cognitive semantics, which experts help to create. The actual practice has shown that the process of model building can be costly and long term. An analysis of relevant big data (BD) can help to automate the process of cognitive modelling. There are two directions of automation: a) verification of cognitive models and b) synthesizing ones. The author's convergent approach based on the inverse problem-solving method and the genetic algorithm for decision-making on the cognitive model was applied. It helps to make the process of cognitive modelling more purposeful and stable. An experimental test and actual practice application of the approach have shown a high level of the models' verifications accuracy (about 93%) but a low level of accuracy of models synthesizing (about 34%). One of the reasons for such a low result lies in the fact that representatives of economic sectors and the digital industry often use different terminologies.

Keywords Artificial intelligence · Big data · Cognitive modelling · Convergent approach · Economic sectors' needs

A. Raikov (✉) · A. Ermakov
Institute of Control Sciences, Russian Academy of Sciences, 117997, Profsoyuznaya st., 65, Moscow, Russia
e-mail: alexander.n.raikov@gmail.com

A. Merkulov
Uchi.Ru LLC, Rochdelskaya st., 15, bldg. 19/20, 123022 Moscow, Russia
e-mail: sasha@merqlove.ru

S. Panfilov
Federal Budget-Financed Institution, "Federal Resources Centre", Staraya Basmannaya st., 11/2, bldg 1, 105064 Moscow, Russia
e-mail: serelen@list.ru

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_20

1 Introduction

The revealing economic sectors' needs in digital technologies are expensive and take a lot of time. There are many economic sectors, the speed of technological progress is high, which cause companies to repeat studying the market some times a year under different angles of vision. This process is ill-defined, and as usual, it requires remote expert participation. Methods of statistical analysis and computer modelling are usually applied. But statistical data and models may be mistaken, which can give excessive risks of planning corporate product policy. It is necessary to consider non-formalized factors, such as business and human preferences and socio-cultural environment.

In such conditions, cognitive modelling [1] helps to represent situations at a qualitative level in the form of concepts (factors) and mutual influences between them. This modelling provides an opportunity to consider the changes in the corporate product policy and evaluate possible development scenarios.

A high barrier to determining the needs of economic sectors in digital technologies lies in the fact that representatives of the economic sectors, on the one hand, and the digital industry, on the other, often use different terminology. The formers use more natural and professional industry vocabulary, whilst the latter present their suggestions in the language of discrete representations, mathematics, digital systems, and services.

This paper is the development of our previous works [2, 3] of assessments of the needs of the economic sectors in digital technologies with trying using cognitive modelling. It is devoted to automatically creating cognitive models using deep learning and analysis of big data (BD). The paper takes into consideration the difference between terminologies of economic sectors' consumers and developers of digital technologies.

2 Terminological Gap

The terminology of the digital sector of the economy differs from the terminology of other sectors of the economy. For example, the livestock industry uses a vocabulary from which the need for digital technology is challenging to identify. The verbal context of the livestock industry is dictated, for example, by terms related to the consumption of drinking milk. Export success is influenced by quality criteria, lead times, and product freshness. The weakening of selection and genetic activity leads to the displacement of pedigree products, their replacement with foreign genetic resources, the cost of which is constantly growing. In this example, the use of digital technologies is indirectly fixed in the following terminology:

- breeding history of animals is lost on import,
- there are no world generalizations of works in the field of genetics,
- forms of breeding certificates are different in different countries, etc.

In the digital economy, the terminology is different. A digital platform creates good conditions for communication, integrates end-to-end digital technologies, and provides digital services. The digital platform is a set of digital services that facilitate interaction between different users over the Internet. The digital platform, for example, provides

- exchange of values between participants,
- conducting transactions that fix a sale of goods,
- processing of information about the conclusion of agreements, etc.

As the thematic fields of the livestock and digital industries are very different, the question arises of building a terminological bridge between the sectors of the economy.

3 Existing Approaches

The market environment analysis is usually carried out by referring to Websites, interviewing experts, etc. For example, in work [4], the industry's need for a particular product is characterized by market demand and potential. In [5], events are recorded that may affect the needs analysis results: market size, competition, inflation, regulation, social change, etc. The market is segmented. The quality functions deployment method helps represents market segments by requirements' characteristics [6, Sect. 2.5].

The analytical system [7] provides an opportunity to compare the availability of joint research in different subject areas. So, upon request to an array of about 230 economic journals (the first quartile, Q1), this system showed a complete lack of intersection of scientific works in creating decision support systems and the agro-industrial sector.

Given the impossibility of a complete and formalized description of the needs for a particular product or service, new marketing methods are increasingly using social and psychological techniques. In this regard, the concept of cognitive marketing appeared. Significant in this approach is the attempt to build appropriate consumption standards. However, this approach is still poorly formalized and do not have automation tools.

Such an analysis demonstrates the development of existing approaches to researching market needs by combining traditional marketing methods and digital technologies, including procedures for analyzing big data and AI. It has to be taken into account that the context that reflects the need of each industry for digital technologies is predominantly cognitive, latent, and indirect. Therefore, cognitive modelling helps to formalize marketing processes, and its high labour intensity requires automation.

4 Automating of Cognitive Modelling

Cognitive modelling helps to support decision-making when qualitative concepts (factors) are more important than quantitative ones. It uses qualitative factors and relations between ones. The nodes represent factors, and arrows – relations between them. Cognitive models can be built semi-automatically and by experts. For example, fuzzy cognitive map (FCM) approaches combine elements of fuzzy logic and neural networks. This approach has been orienting on automatically creating FCM [8, 9].

The retrospective information helps to automate the models' building by mapping cognitive models' factors on the relevant subsets of BD. But it helps only to verify cognitive models which experts make. The use of deep learning of the neural network with long short-term memory method was suggested for automating cognitive modelling for emergencies, but this idea was not tested [3].

This work used an array of about 200,000 relevant documents (news, article, etc.) from electronic media for each vertex of the cognitive model for training a deep neural network. The trained neural network was used to classify media documents based on cognitive model factors. Using a neural network made it possible to eliminate from the sequence of constructing a cognitive model the procedures for formulating search queries and referring to BD for these queries. The process of collecting, processing, and presenting data included the following stages:

1. Determination of the boundaries of information search, selection of sites.
2. The choice of the format of interaction with the data of sites on the Internet.
3. Collecting the full news stream.
4. Processing the collected data (classifying documents using a neural network).

At stage (1), the criteria related to the required group of Internet sources, the data from which are subject to analysis, are determined: a segment or a group of Internet segments, the depth of the retrospective of the analyzed data, etc.

At stage (2), the interaction format with Internet data is determined under the established boundaries of information retrieval. The interaction format is implemented in an automated mode using the search capabilities of modern Internet aggregators.

At stage (3), the news flow was collected from selected sites related to a given topic (for example, the "agriculture" industry). At the moment, the created sample of sites includes:

- digital news sources (habrahabr.ru; cnews.ru; computer-ra.ru, etc.),
- federal and regional media (vesti.ru; newsru.com; regions.ru, etc.),
- unique sources of industry (industrialnews.ru; agbz.ru; agri-news.ru, etc.).

At stage (4), an automatic classification of media documents was performed according to the features of specific vertices of the cognitive model. In the future, each class of documents is processed with an analysis of their text content.

Several experiments have been conducted using recurrent neural network (RNN) and convolutional neural network (CNN). For the CNN, an approach with word coding helped to classify texts. A vector of fixed length was associated with each word, then a matrix of vectors was fed to the CNN input. The method for translating a word into a fixed length vector was Google's Word2Vec technology. The implementation of neural networks was made using the Python 3.7 programming language and the Keras library in conjunction with the TensorFlow framework. The algorithm of classification of the input stream from media sources used the following factors of the cognitive model:

- "Compliance with the world's best solutions (innovativeness)",
- "Prospects for the commercialization of new technologies",
- "Breakthrough nature of technical solutions (export-oriented)".

The size of the training samples for the above factors was 8000, 12,000, and 5600 documents, respectively. The test sample size was 100,000 media documents in Russian for the period from the beginning of 2021.

Testing was performed under various conditions determined by the maximum number of words in the test document (200 or 500) and the maximum number of words in the encoding dictionaries (2000; 5000; 7000). The number of learning epochs for each neural network was at most 20. Classification results were estimated using the "accuracy" metric, i.e. the proportion of correctly classified documents to their total number was counted. Figures 1 and 2 show examples of using RNN and CNN in different conditions. The "accuracy" parameter reflects the value of the classification accuracy function: "val_accuracy"—classification accuracy at the training stage, "accuracy"—during testing. The number of learning epochs is represented on the graphs by the "epochs" parameter.

The reason for the low-quality level of classification is:

- prominent intersection of documents corresponding to different factors,
- difference in professional terminology in the economic sectors,
- need to solve the inverse problem with inclusion of a person in process.

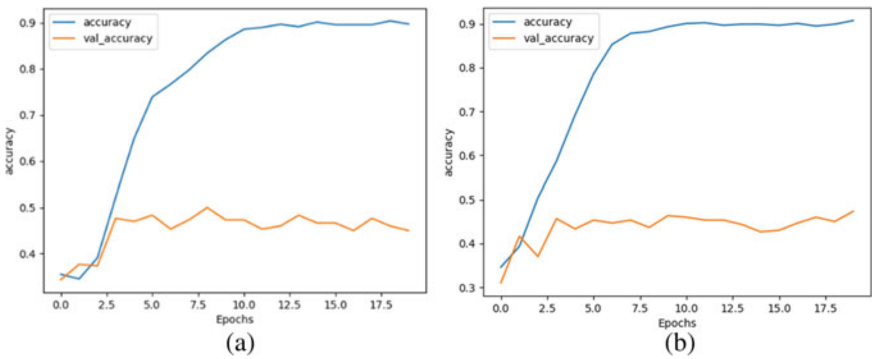


Fig. 1 Plots of "accuracy" distribution for RNN for 20 learning epochs: **a** the maximum number of words in a document—500 and vocabulary size—2000 words; **b** the maximum number of words in a document is 200, and the size of the vocabulary is 5000 words

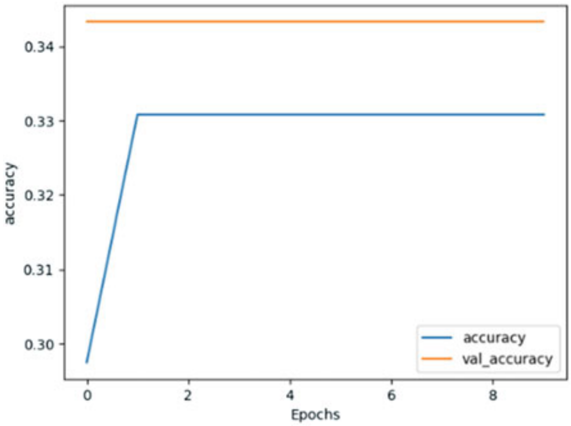


Fig. 2 Graphs of "accuracy" for CNN for 10 learning epochs with the maximum number of words in the document—450 and the volume of the vocabulary—7000 words

The well-known linguistic methods can help to eliminate terminological causes, but refusal to include a person in the process of solving the inverse problem can go along the path of developing strategies for solving such problems.

5 Quasi-solution of Inverse Problem

The quasi-solution of the inverse problem on a cognitive model was developed by using a genetic algorithm. Experiments have shown that the inverse problem solutions become unstable even to small perturbations of the control action.

A 2-level regularization was applied to increase the stability of the inverse problem-solving. It helped analyze the neighbourhood of optimal solutions at the first level and improve the quality function by including additional components that directly depend on the control action at the second level. The quality functional of solving an inverse problem on a cognitive graph can be represented as follows:

$$f(u_k) = \frac{1}{N}\sum_{j=1}^{N}\left(\sqrt[2]{\sum_{i}(T_i(j) - X_i(u_k, j))^2}\right) \tag{1}$$

where N is the number of steps in modelling the direct problem, j—is the step in modelling the direct problem, i—is the index of the target factor, $T_i(j)$—is the target value of the target factor i at the step j of modelling the direct problem, $X_i(u_k, j)$—is the calculated value of the target factor i at the step of modelling j of the direct problem, u_k—is the value of the control action k for which the quality functional is calculated. Usually, in cognitive modelling, the control action u_k is an impulse of a certain magnitude.

The range of possible values of the control action u_k, and the number of control factors in the model determines the search space on which the solution of the inverse problem is carried out. Various values of the control actions u_k are analyzed during optimization due to functional (1), whilst the optimization task is to determine such a control value u_k, at which this functional will take a minimum value, which corresponds to the minimum discrepancy between the target values and the calculated ones.

A feature of evolutionary optimization methods is the appearance in the composition of the populations of many specimens of decisions corresponding to close to optimal values of the quality function. In the usual classical practice, the recalculation of the functional (1) values for the known values of u_k is not performed. At the same time, there is a high probability of obtaining unstable solutions. It is proposed to repeat the calculation of functional (1) to eliminate these solutions for the previously calculated values of u_k. It is also proposed to apply an additional random control action from the range determined by the required stability characteristics of the solution of the inverse problem to the previously analyzed values of the control actions u_k, as a regularizer. In this case, the quality functional (1) calculated for the control action u_k is averaged over all the calculated points of the neighbourhood. Thus, insufficiently stable solutions will have the worst averaged values of the quality functional (1) in the vicinity of the control u_k, even if the functional (1) is minimal directly at the point u_k. Parameters of the optimization algorithm (for example, the parameters of the elitism operator and the selection operator) determined the number of solutions calculations in the neighbourhood.

The quality functional (1) does not analyze the direct values of the control actions; accordingly, in the case of the same values (1) for the edge values of u_k, the result of the algorithm is unpredictable. An introduction of an additional regularization coefficient into the functional (1) eliminated this limitation. Then, the functional will have the following form:

$$f(u_k) = \frac{1}{N}\sum_{j=1}^{N}\left(\sqrt[2]{\sum_i (T_i(j) - X_i(u_k+\varepsilon, j))^2}\right) + \delta\sqrt[2]{\sum_l \left(u_k^l\right)^2}, \tag{2}$$

where ε—is a random control action from the range determined by the required stability characteristics of the solution to the inverse problem. As a rule, $|\varepsilon_l| \ll \left|u_k^l\right|$, δ—is the control action regularization coefficient, is determined experimentally, l—are the indices control factors of the cognitive model.

The proposed approach to solving the inverse problem makes it possible to reduce human participation at intermediate stages (populations) of the genetic algorithm execution. The decision-maker only evaluates the final decision. And if this solution does not suit him, the genetic algorithm can offer another way to achieve the given goal of solving the problem.

6 Practical Advantage

The practical advantage of applying the suggested approach consists of increasing the competitiveness of products and services in domestic and global markets, raising labour productivity by implementing information technology and AI, purposeful formation of digital value chains, and developing the interaction of different industries.

The unique convergent automation of research of a rather complex segmented market helps to accelerate to revealing economic sectors' needs crucially. Our paper [2] represents the process of assessments of the needs of the economic sectors in digital technologies without using neural networks, which already showed positive results in actual practice.

7 Limitations and Discussion

The limitations of the work are seen in the impossibility of automatically taking into account the non-formalizable and uncaused cognitive semantics of AI models. They show the direction of the scientific discussion issues in the future. The group of experts can represent such semantics. The paper describes the approach with mapping factors of AI models to big data and applying the inverse problem-solving method with genetic algorithm. It helps to take into consideration the cognitive semantics and make the decision-making process more purposeful and sustainable. Some results can be seen in [10].

8 Conclusion

The results of this work allow us to draw the following conclusions:

- it was possible to ensure the value of the accuracy of the classification of factors for the cognitive model using both RNN and CNN only 34%,
- the objective reason for the relatively low level of the classification quality is the need to solve the inverse problem, which requires the inclusion of a person in the solution process who must make intermediate estimates,
- the reason for the relatively low quality of the results of the classification of factors using neural networks was also the prominent intersection of articles (duplication) corresponding to different factors of the model, as well as the difference in professional terminology in the sectors of the economy.

The main options for improving the quality of classification of factors for the automatic construction of a cognitive model are as follow:

- identification of factors of the cognitive model by both mapping them to big data and neural networks,
- development of a mechanism for eliminating overlapping data in training samples,
- creating the linguistic bridge between digital and different economic sectors terminologies,
- modification of the algorithm for solving the inverse problem with the connection of a person only to assess the final results of the solution.

In our opinion, this study will have a crucial impact on developing marketing technologies in the long run by making them more accurate, purposeful, and cheap.

Acknowledgements Russian Science Foundation, grant No. 21-18-00184.

References

1. Avdeeva Z, Kovriga S (2008) Cognitive approach in simulation and control. In: Proceedings of the 17th world congress “The International Federation of Automatic Control”, Seoul, Korea, 6–11 July, pp 1613–1620. https://doi.org/10.3182/20080706-5-KR-1001.00275
2. Raikov AN, Ermakov AN, Merkulov AA (2019) Assessments of the economic sectors needs in digital technologies. Lobachevskii J Math 40(11):1837–1847. Pleiades Publishing, Ltd. https://doi.org/10.1134/S1995080219110246
3. Raikov AN (2020) Accelerating decision-making in transport emergency with artificial intelligence. In: Second international virtual conference on multidisciplinary research 2020. Adv Sci Technol Eng Syst J (ASTESJ) 5(6):520–530. https://doi.org/10.25046/aj050662
4. Sarin S (2013) Business marketing: concepts and cases. McGraw Hill Education (India) Private Limited, New Delhi, India, p 654
5. Stevens RE, Sherwood PK, Dunn JP (2006) Market opportunity analysis: text and cases. best business books. Imprint of The Ha Worth Press, Inc. New York, London, Oxford. Psychology Press, p 263
6. Gubanov D, Korgin N, Novikov D, Raikov A (2014) E-expertise: modern collective intelligence. Springer. Series: studies in computational intelligence, vol 558, p XVIII. https://doi.org/10.1007/978-3-319-06770-4
7. VOSviewer, https://www.vosviewer.com/. Accessed 12 Oct 2021
8. Axelrod RM (1976) Structure of decision: the cognitive maps of political elites, the structure of decision the cognitive maps of political elite. Princeton University Press, p 404
9. Karatzinis GD, Boutalis YS (2021) Fuzzy cognitive networks with functional weights for time series and pattern recognition applications. Appl Soft Comput 106:107415. https://doi.org/10.1016/j.asoc.2021.107415
10. Raikov A (2021) Cognitive semantics of artificial intelligence: a new perspective. Springer Singapore, topics: computational intelligence XVII. https://doi.org/10.1007/978-981-33-6750-0

Prototype Based on a LoRaWAN Network for Storing Multivariable Data, Oriented to Agriculture with Limited Resources

Steven Castro, Jhonattan Iñacasha, Gustavo Mesias, and William Oñate

Abstract Due to the advancement in information digitization in the agricultural area that has resulted in processes which are more intelligent and independent of precision agriculture, having as objective the verification, quantification, calculation, processing, and storage of variables immersed in the agricultural area, the present work shows a LoRa sensors network system, with visualization in a cloud environment through The Things Network and data analysis in an IoT platform called ThingSpeak. The objective of the use of sensors in precision agriculture (PA) is to measure the different environmental parameters (e.g., temperature, humidity, soil pH value), which are sent through a LoRaWAN gateway that receives the variables sensed by the final nodes and in turn incorporates a specialized node based on artificial vision to obtain the vegetation index. In addition, a comparison with a commercial datalogger is carried out, achieving an average error of 3.67% in the measured variables and a cost 17 times smaller in the design of the proposed system.

Keywords LoRaWAN · TTN · ThingSpeak · Datalogger

1 Introduction

Information digitization in the agricultural area has enabled optimization of processes, which have become individualized and intelligent, since as mentioned in [1], these processes operate in real time, obtaining precise information about the

S. Castro (✉) · J. Iñacasha · G. Mesias · W. Oñate
Universidad Politécnica Salesiana, Quito, Ecuador
e-mail: scatroj@est.ups.edu.ec

J. Iñacasha
e-mail: gmesias@ica.csic.es

G. Mesias
e-mail: jinacasha@est.ups.edu.ec

W. Oñate
e-mail: wonate@ups.edu.ec

Universidad Politécnica de Madrid, Madrid, España

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_21

cultivation areas, which are now managed by a new entity with the role change from farmer to agro-manager. With the help of IoT (Internet of Things) devices, it is appropriate to collect data at any instant of the agricultural production process. These are transmitted by wireless sensor networks through the machine to machine (M2M) support platform [2]. This is possible by incorporating different architectures, which consist of IoT devices, sensor networks, edge devices, edge computing [3], and also include cloud services for data storage, visualization, and management, all of which has enabled the availability of automated systems, taking a step forward and transforming it into Agriculture 4.0 [4].

From the aforementioned, technology has undoubtedly been the protagonist in the evolution of agriculture, having as objective the verification, quantification, calculation, processing, and storage of variables immersed in the agricultural area [5], thus that the digitized data are now available for advanced analytics at any moment and at any place.

At present, there are different infrastructure topologies based on the requirements of the process, and thus, [6] proposes a structured bidirectional architecture of IoT devices with radiofrequency communication (analog signal, digital, and pulses), edge devices (MCU), fog devices (Gateway), and visualization in a cloud environment. A unidirectional architecture with network of sensors using LoRa and Zigbee communication protocol is proposed in [7], for measuring temperature and humidity.

The evolution of technology and image processing techniques has contributed to implement in agriculture vegetation indices that enable detecting and highlighting cultivation areas among other elements present in a particular area [8]. Vegetation indices are reflectance measures of various wavelengths, which combined in different ways enable obtaining agricultural features such as vegetation coverage, biomass production, plant identification, and health [9]. An example of a research work currently underway is the Normalized Difference Vegetation Index(NDVI) with visible light and near infrared (NIR) and the Color Index of Vegetation Extraction (CIVE) with visible spectra, such studies have shown good results [10]. However, these methods were not used in a data collection architecture at any instant and at any place, as well as in our particular case in which a LoRa network with low consumption sensors is implemented, that enable measuring various variables such as environmental temperature, soil temperature, environmental humidity, soil humidity, atmospheric pressure, solar radiation, luminous intensity and Vegetation Index, with the latter being a sensor with artificial vision, that captures the image within the visible spectrum (RGB), for determining the Vegetation Index (CIVE) [11] in a cultivation area. The data acquired are sent to a cloud data structure so that the agro-manager performs the statistical analysis according to his/her convenience, thus contributing to the standards demanded by Precision Agriculture ag4.0 [12].

2 Methodology

2.1 *LoRaWAN Gateway*

A gateway was implemented to enable final nodes to connect to the Internet through LoRaWAN communication, for which it used an HT-M00 dual-channel LoRa gateway module. This gateway is based on two SX1276 chips driven by ESP32 [13], thus enabling the expansion of minimum interference communication and low energy consumption for LoRa. The frequency of the sensor network developed in this study was established according to the geographic location for synchronization with the server IP, and finally, it was created a The Things Network (TTN) console to enable the gateway by sending the ID [14].

2.2 *Nodes*

Each LoRa network node is composed of an ESP32 microprocessor (dual-core 32 bit The Wi-Fi Lora 32 (V2) with ESP32 and SX127 [15] enables connecting the LoRaWAN at 915 MHz (range from 902 to 928 MHz) for the Americas region [16]. Table 1 shows the sensors connected to each node in the sensor network.

The MCCI LORAWAN LMIC TTN-ABP library (activation by personalization) developed in the Arduino ID, enables communication between node 1, node 2, or node 3 and the TTN page, where the following parameters were configured: network session key, application session key, and device address, which were obtained by TTN [17].

Algorithm 1 shows the modification of the GPIOs PIN MAPPING for configuring the nodes in the connection with LoRa.

Table 1 Devices of the LoRaWAN sensor network

Node 1		Node 2		Node 3	
Sensor	Model	Sensor	Model	Sensor	Model
Soil temperature	DS18B20 (probe)	Environmental temperature	DHT -22	Vegetation Index	Camera rev 1.3
Soil humidity	FC-28	Environmental humidity		(Artificial vision)	
Atmospheric pressure	BMP180	Solar radiation	ML8511		
Luminous intensity	BH1750				

Algorithm 1 GPIOs PIN MAPPING Configuration

```
Input: nss, rxtx, rst, dio
Output: GPIOs pin mapping
1: gpio 18 $\leftarrow$ nss
2: LMIC_UNUSED_PIN $\leftarrow$ rxtx
3: gpio 14 $\leftarrow$ rst
4: gpio 26, 35, 34 $\leftarrow$ dio
```

Different functions and libraries were used for sending the sensed data from the nodes to TTN, for transforming the data read in bits per frame for its further transmission, as it is the case for the BMP180 sensor in which 3 main libraries were used for its operation: Adafruit_Sensor, Adafruit_BME280 and SFE_BMP180, the DS18B20 sensor, in which two main libraries were used for its operation: OneWire and DallasTemperature, the BH1750 sensor, in which two main libraries were used for its operation: Wire and BH1750, the FC-28 sensor used a mapping of the reading from an analog pin, the DHT-22 sensor, in which a DHT library was used, and for the Camera rev 1.3 sensor, it was used the OpenCv (Open Source Computer Vision) library.

The sensed data is read using the do_sense function in the Arduino ID, and subsequently, these data are sent to the LoRaGateway using the do_send function, as it is observed in Algorithm 2.

Algorithm 2 Frame for sending sensor data

```
Input: Humidity, temperature, uvIntensity, VI
Output: LMIC_setTxData2
1: int shiftHum $\leftarrow$ int(Humedad * 100)
payload[0] $\leftarrow$ byte(shiftHum)
payload[1] $\leftarrow$ shiftHum >> 8
2: int shiftTemp $\leftarrow$ int(temperatura * 100)
payload[2] $\leftarrow$ byte(shiftTemp)
payload[3] $\leftarrow$ shiftTemp >> 8
3: int shiftUV $\leftarrow$ int(uvIntensity * 100)
payload[4] $\leftarrow$ byte(shiftUV)
payload[5] $\leftarrow$ shiftUV >> 8
4: int shiftVI $\leftarrow$ int(VI * 100)
payload[6] $\leftarrow$ byte(shiftVI)
payload[7] $\leftarrow$ shiftVI >> 8
```

2.3 Method of Vegetation Index (Sensor with Artificial Vision)

The RGB image sensor (PiCamera) is enabled and configured in the Raspberry Pi Zero, and the OpenCV (Open Source Computer Vision) library is used for image analysis and treatment.

The processing initiates capturing and storing the RGB image with a size of 720 × 720 pixels of the cultivation area, from which the undesired features are eliminated, and it highlighted the area of interest through the implementation of the CIVE (Color Index of Vegetation Extraction) algorithm [18], whose main function is extracting the vegetation from the image emphasizing green areas [19]. The Otsu

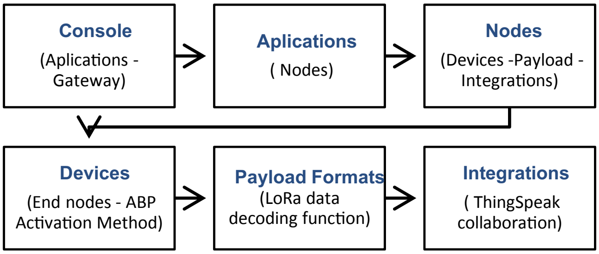

Console
(Aplications - Gateway)
Aplications
(Nodes)
Nodes
(Devices -Payload - Integrations)
Devices
(End nodes - ABP Activation Method)
Payload Formats
(LoRa data decoding function)
Integrations
(ThingSpeak collaboration)

Fig. 1 Steps for configuring the nodes in TTN

thresholding method was used for obtaining the binary image (Boolean matrix), obtaining a representation with a pixel value of 1 for the white part and a value of 0 for the black part. Equation (1) was used to determine the vegetation percentage present in the image of the cultivation area.

$$\mathrm{VI} = \frac{\sum_{i,j=1}^{n} a_{i,j}}{518400} 100\% \tag{1}$$

The value of Vegetation Index percentage is sent from the Raspberry Pi Zero to the analog input of the LoRa node; signal conditioning was previously performed.

2.4 Configuration of Nodes in TTN

Figure 1 shows the configuration steps carried out in the TTN application for each node, thus establishing the communication between nodes and TTN, stressing that each application has a similar ABP activation method. Nevertheless, the parameters are different and designated by TTN (e.g., for node 1, the parameters designated from TTN are: device EUI: 00 8A 2F 9E 2F 39 A7 15, application EUI: 70 B3 D5 7E D0 03 EE C8, and device address: 26 01 1B 8D), which were used for configuring the ID of each node, thus establishing the aforementioned communication.

2.5 Data in Payload TTN

The data sent by the nodes were decoded in TTN cloud environment for identification in the payload of each sensed variable. Different fields were created in this platform for each variable, with which a key is generated by means of an API to access a channel, where the agro-manager is in charge of managing such access, thus achieving the writing of the sensed values in the ThingSpeak IoT service platform.

Algorithm 3 Decoding in TTN of node 2

```
Input: b, port
Output: Humidity, temperature, uvIntensity
var Humidity = (b[0] | b[1] << 8)/100;
var temperature = (b[2] | b[3] << 8)/100;
var uvIntensity = (b[4] | b[5] << 8)/100
return {
field1: Humidity + " %",
field2: temperature + " °C",
field3: uvIntensity + " mW/cm$^2$"}
```

Algorithm 3 shows an example corresponding to the decoding of sensed values from node 2 in TTN and the use of fields for identifying the variables of interest.

2.6 Collaboration with ThingSpeak

For treatment and visualization of the data obtained through TTN, 3 channels were created with the sensors used in each final node by means of a collaboration with an IoT platform [20], which enabled collecting, saving, and making easier for the agro-manager to perform data analytics at any instant and at any place [21].

Figure 2 shows the block diagram of the LoRaWAN network architecture developed for the measurement of the different physical variables, where the nodes communicate with the gateway using LoRa technology, the gateway sends the LoRaWAN frames to a cloud platform for the processing of the detected data [22].

3 Results

Data were collected in a cultivation area of 1120 [m2], as shown in Fig. 3, in which node 1 is in charge of taking data of soil temperature (DS18B20), soil humidity (FC-28), luminous intensity (BH1750), and atmospheric pressure (BMP180); node 2 is designated for taking data of environmental temperature (DHT22), environmental humidity (DHT22) and solar radiation (ML8511), and node 3 takes data of Vegetation Index by means of artificial vision through a camera.

Due to the nonpriority time of the process, data were sent from the nodes to the TTN platform approximately every 12 s. Table 2 shows an example of the record of values in TTN from node 2, showing the payload in the process information fields in hexadecimal format (environmental humidity, environmental temperature, and solar radiation).

Afterward, the variables measured are recorded through the ThingSpeak page, and such platform enables the agro-manager to graphically visualize data representation at any instant and at any place, also having a record of historic data and access to statistical tools for the corresponding analytics. Figure 4 shows two widgets as an

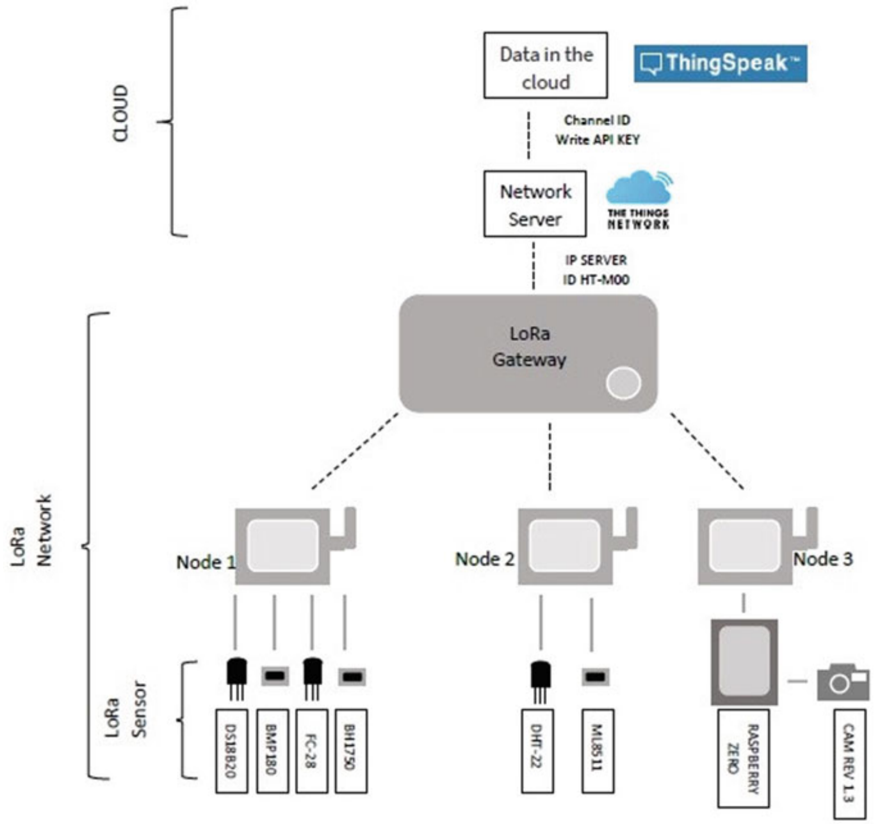


Fig. 2 LoRaWAN network architecture

Fig. 3 Cultivation area located in the city of Quito latitude: −0.172889 and longitude: −78.332341

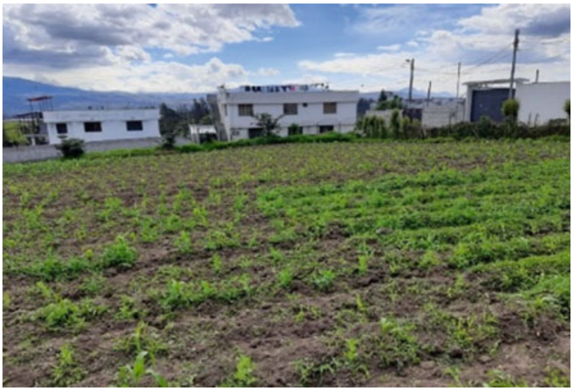
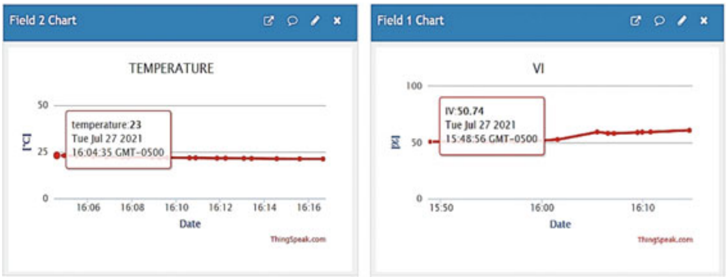


Table 2 Information fields recorded in TTN from node 2

Time	Counter	Port	Payload	Field 1 (%)	Field 2 (°C)	Field 3 (mW/cm^2)
15:58:42	730	1	CC 10 62 0C 29 01 00 00 00 00 00 00	43	31.7	2.97
15:58:21	726	1	D6 10 62 0C 64 01 00 00 00 00 00 00	43.1	31.7	3.56
15:58:01	722	1	CC 10 62 0C 5D 01 00 00 00 00 00 00	43	31.7	3.49
15:56:44	707	1	4E 11 4E 0C 5D 01 00 00 00 00 00 00	44.3	31.5	3.49
15:56:19	702	1	BC 11 62 0C 63 01 00 00 00 00 00 00	45.4	31.7	3.55
15:55:17	690	1	A2 12 A8 0C 7D 01 00 00 00 00 00 00	47.7	32.4	3.81



(a) (b)

Fig. 4 Record and visualization of data of **(a)** environmental temperature and **(b)** vegetation

example, for values of environmental temperature and Vegetation Index stored in the field by means of a dispersion graph.

The platform under consideration enabled downloading the data taken during the field test in different formats (JSON, XML, and CSV), and thus, Table 3 shows the average values obtained during the cultivation process.

4 Discussion

Since agriculture and livestock are located in places with low coverage, it is appropriate to use some type of wireless technology that enables the connection of various sensors for precise measurement of its variables. Consequently, there are various companies that offer modules and systems with wireless technology; however, their implementation involves a high cost; thus, this study reveals various comparative

Table 3 Average data collected from ThingSpeak

Node 1		Node 2		Node 3	
Average		Average		Average	
Soil temperature (°C)	22.28	Environmental temperature (°C)	26.07	Vegetation Index (%)	42.68
Soil humidity (%)	40.6	Environmental humidity (%)	39.79		
Luminous intensity (lm)	26,269	Solar radiation (mW/cm^2)	1.31		
Atmospheric pressure (mbar)	755.4				

aspects between two wireless systems, one commercial and another developed in this study. The points of interest are focused in the same area of analysis for cultivation, cost, refresh rate, data storage in the cloud and number of variables to be measured.

The wireless HOBO MicroRX commercial station with IEEE 802.15.4 technology has the low cost as parameter of interest in its description, enabling the connection of up to five plug-and-play sensors at level of research, with these being environmental temperature, soil temperature, environmental humidity, soil humidity, luminous intensity, solar radiation, and atmospheric pressure, and also enables the user to visualize and download the stored data from the HOBOnet platform. A peculiarity of this company is that it enables to store data at intervals from 1 s to 30 min. From the aforementioned specifications, some issues arise regarding cost, since a wireless technology such as the LoRaWan at the level of research considered in this case study with the same sensed variables has an approximate cost 17 times smaller compared to the commercial one. It should be stressed that the sensors used in the commercial system show a lower measurement error, as specified in Table 4.

It is observed in Table 3 that the mean error values in the low-cost system might be adjusted to minimize the error; however, the solar radiation variable shows a larger error margin, since the commercial sensor has a larger spectral coverage of the rays that fall upon the surface of earth, which range approximately between 300 and

Table 4 Mean percentage error between the system developed in this study and the commercial system in 12 h

Mean percentage error	
Environmental temperature (%)	4.68
Environmental humidity (%)	3.02
Soil temperature (%)	4.33
Soil humidity (%)	3.11
Atmospheric pressure (%)	2.76
Solar radiation (%)	46.09
Luminous intensity (%)	4.12

3500 nm [23], with respect to the low-cost sensor with measures wavelengths between 280 and 390 nm. The system developed in this study presents a unique interval of data storage every 15 s, due to the type of process on which the system was installed, i.e., it does not require a constant data update or priority times, and this interval may be even larger, such measured data are transmitted to a Web platform, where the agro-manager may visualize and perform the corresponding analytics. It is also mentioned that the system under consideration consists of a low-cost specialized node for obtaining the Vegetation Index of the cultivation area, through artificial vision, and finally, it is important to mention that the line of sight of the LoRaWan technology is larger than the technology in the commercial system and unquestionable the easiness of implementation of the aforementioned two systems.

5 Conclusions

The system developed in this process fulfills satisfactorily the proposed goals, which means that the agro-manager may manage from any place and at any moment the variables involved in the cultivation process, which are soil temperature, soil humidity, environmental temperature, environmental humidity, luminous intensity, atmospheric pressure, and solar radiation. The aforementioned variables were sensed through devices that showed an average measurement error of 3.67% with respect to the commercial datalogger; however, a high average error was obtained in the solar radiation variable, since the sensor only measures 3.44% of the total radiation range that reaches Earth.

The system has features that enable adding sensing devices from different manufacturers and is not limited to proprietary sensors as various commercial dataloggers. The system is also constituted by nodes that take part of the LoRa network which are of low-cost. It is also mentioned that the precision agriculture system developed in this paper has an additional artificial vision sensor for obtaining the Vegetation Index. These qualities highlight even more because it was achieved an economic cost 17 times smaller compared to the commercial datalogger.

References

1. La EN, Las AY, Rurales Z (2019) Tecnologías digitales. Tecnol Digit. https://doi.org/10.2307/j.ctvt6rmh6
2. Zhao JC, Zhang JF, Feng Y, Guo JX (2010) The study and application of the IOT technology in agriculture. In: Proceedings of 2010 3rd IEEE international conference on computer science and information technology ICCSIT 2010, vol 2, pp 462–465. https://doi.org/10.1109/ICCSIT.2010.5565120.
3. Nguyen Gia T, Qingqing L, Pena Queralta J, Zou Z, Tenhunen H, Westerlund T (2019) Edge AI in smart farming IoT: CNNs at the edge and fog computing with LoRa. IEEE AFRICON conference, vol 2019-Sept, no September 2019. https://doi.org/10.1109/AFRICON46755.2019.9134049

4. Liu Y, Ma X, Shu L, Hancke GP, Abu-Mahfouz AM (2021) From industry 4.0 to agriculture 4.0: current status, enabling technologies, and research challenges. IEEE Trans Ind Inf 17(6):4322–4334. https://doi.org/10.1109/TII.2020.3003910
5. Cisternas I, Velásquez I, Caro A, Rodríguez A (2020) Systematic literature review of implementations of precision agriculture. Comput Electron Agric 176:105626. https://doi.org/10.1016/j.compag.2020.105626
6. Lozoya C, Aguilar A, Mendoza C (2016) Service Oriented design approach for a precision agriculture datalogger. IEEE Lat Am Trans 14(4):1683–1688. https://doi.org/10.1109/TLA.2016.7483501
7. Ali AI, Partal SZ, Kepke S, Partal HP (2019) ZigBee and LoRa based wireless sensors for smart environment and IoT applications. In: Proceedings of 2019 IEEE 1st global power, energy communication conference GPECOM 2019, pp 19–23. https://doi.org/10.1109/GPECOM.2019.8778505
8. Kim Y, Oh J, Choi J, Kim Y. Comparative analysis of the hyperspectral vegetation index and radar vegetation index : a novel fusion vegetation index. Department of Civil and Environmental Engineering , Seoul National University , Republic of Korea Department of Civil Engineering, C, pp 1–4
9. Zhao H, Li Y (2020) Monitoring monthly soil moisture conditions in China with temperature vegetation dryness indexes based on an enhanced vegetation index and normalized difference vegetation index
10. Suarez PL, Sappa AD, Vintimilla BX (2018) Learning image vegetation index through a conditional generative adversarial network. In: 2017 IEEE second ecuador technical chapters meeting ETCM 2017, vol 2017-Jan, no 1, pp 1–6. https://doi.org/10.1109/ETCM.2017.8247538
11. Kataoka T, Kaneko T, Okamoto H, Hata S (2003) Crop growth estimation system using machine vision. In: IEEE/ASME international conference on advanced intelligent mechatronics, AIM, vol 2, no Aim, pp 1079–1083. https://doi.org/10.1109/AIM.2003.1225492
12. Wiangtong T (2020) IoT-based versatile platform for precision farming. In: 2018 18th International symposium on communications and information technologies no. ISCIT 2018, pp. 438–441
13. Lavric A, Petrariu A (2018) LoRaWAN communication protocol : the new era of IoT. pp 74–77
14. Barro A. TLTN—The local things network : on the design of a LoRaWAN gateway with autonomous servers for disconnected communities, pp 1–4
15. Wang J (2019) Design and implementation of small monitoring wireless network system based on LoRa IAEAC, pp 296–299
16. Buyukakkaslar MT, Erturk MA, Aydin MA, Vollero L, Campus U, Roma B (2017) LoRaWAN as an e-health communication technology. https://doi.org/10.1109/COMPSAC.2017.162
17. Bernardinetti G (2020) Disconnection attacks against LoRaWAN 1.0. X ABP devices
18. Yang T, Chen Y, Fan Z (2018) Vegetation segmentation based on variational level set using multi-channel local wavelet texture and color. Signal Image Video Process 12(5):951–958. https://doi.org/10.1007/s11760-018-1239-3
19. Hamuda E, Glavin M, Jones E (2016) A survey of image processing techniques for plant extraction and segmentation in the field. Comput Electron Agric 125:184–199. https://doi.org/10.1016/j.compag.2016.04.024
20. Abdul-Rahman AI (2020) Internet of Things application using tethered MSP430 to Thingspeak cloud, pp 352–357. https://doi.org/10.1109/SOSE.2016.42
21. Parida MD (2019) Real-time environment monitoring system using ESP8266 and ThingSpeak on Internet of Things platform. no ICICCS, pp 225–229
22. Hartner R, Tschandl M, Bischof C. Digital shop floor management : a practical framework for implementation
23. De Barros C, Callegari S, Caires W, Amorim S, Silva MP, Pereira HA (2018) Low-cost solar irradiance meter using LDR sensors. In: 2018 13th IEEE international conference industry applications, pp 2–79

Real-Time and Zero-Footprint Bag of Synthetic Syllables Algorithm for E-mail Spam Detection Using Subject Line and Short Text Fields

Stanislav Selitskiy

Abstract Contemporary e-mail services have high availability expectations from the customers and are resource-strained because of the high-volume throughput and spam attacks. Deep machine learning architectures, which are resource hungry and require offline processing due to the long processing times, are not accepted at the front-line filters. On the other hand, the bulk of the incoming spam is not sophisticated enough to bypass even the simplest algorithms. While the small fraction of the intelligent, highly mutable spam can be detected only by the deep architectures, the stress on them can be unloaded by the simple near real-time and near zero-footprint algorithms such as the bag of synthetic syllables algorithm applied to the short texts of the e-mail subject lines and other short text fields. The proposed algorithm creates a circa 200 sparse dimensional hash or vector for each e-mail subject line that can be compared for the cosine or Euclidean proximity distance to find similarities to the known spammy subjects. The algorithm does not require any persistent storage, dictionaries, additional hardware upgrades or software packages. The performance of the algorithm is presented on the one day of the real SMTP traffic.

Keywords Spam detection · Bag of features · Short text · E-mail subject · Online training · Proximity metrics

1 Introduction

Level of the spam e-mail traffic coming through the simple mail transfer protocol (SMTP) [12], circa 90% before or 50% after IP filtering, makes it effectively non-functional without filtering neither for users nor economically sound for the Internet Service Provider (ISP) companies. The majority of the practical anti-spam solutions rely on crowd-sourcing and, partially, expert analysis of the spam-attracting honey-pot accounts to extract signatures from the spam message example. Such signatures

S. Selitskiy (✉)
Earthlink Internet, Atlanta, GA 30328, USA
e-mail: selitsky@yahoo.com

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_22

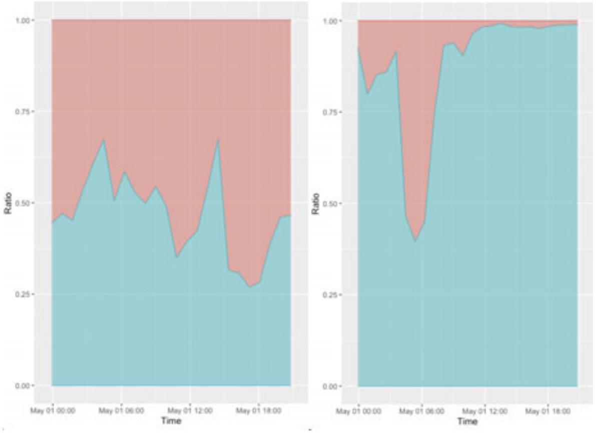


Fig. 1 Left: Spam (bottom) to no spam (top) ratio (after IP filtering). Right: dumb (bottom) to intelligent (top) spam ratio. 24 hours snapshot

include IP addresses, handshake and source domains, header domains, subject and other text headers, body text, URLs, and attachments. Filtering on such signatures is usually effective, in terms of accuracy and speed, against the non-sophisticated spam comprising about 90% of all spam traffic Fig. 1. However, such signatures become available only a few hours after the spam attack with unknown previously signatures starts. Also, keeping and searching database of spam signatures require either significant computing and storage resources on-site or paid subscription to the spam-filtering providers.

Intelligent spammers are aware of these limitations and exploit them by running distributed, short-lived, intense campaigns Fig. 1 right, rotating spam signatures, monitoring the anti-spam algorithms' effectiveness via so-called canary accounts, and crafting unique spam messages individually tailored for each recipient. Deep learning (DL) algorithms can detect sentiment and semantic of the intelligent spam full-body texts [5, 24].

However, DL algorithms require significantly more resources and have longer processing time than simpler algorithms. Although SMTP standards allow plenty of time for a message to be delivered to the recipient, contemporary e-mail users expect near real-time message delivery. Therefore, slow and expensive DL algorithms tend to be used on the last line of the defence for messages with the unclear verdict. Another indirect impact of the full-body message scan has game-theoretic consequences—it increases the incoming spam messages' size up to the maximal limits because spammers try to overwhelm spam filters. Therefore, for employing full-body analysis, ISP should be prepared resource-wise to handle the shifting traffic's structure and volume.

The behavioural-based algorithms use the simplified feature space proximity analysis for the subject line and other short text headers to fill the apparent gap between the static signature-based algorithms and the DL full-body semantic and sentiment analysis algorithms. Bag of words' algorithms are a popular choice for such analysis [25]. They use from the few hundred to few thousand-dimensional spaces of the frequency vocabularies and various distance and class boundary algorithms such as cosine and Euclidean distances, or support vector machines (SVM) and artificial neural networks (ANN) regression algorithms. However, bag of words models require text pre-processing and database infrastructure that consume time and hardware resources.

The presented bag of synthetic syllables (BoSS) algorithm is self-contained, has a straightforward fast-computing logic, does not require any external resources and introduces minimal CPU or memory-wise overhead. The BoSS algorithm can be viewed as related to n-gram algorithms with custom 2-gram and 1-gram mix that creates enough dimensional space to handle short texts, still maintaining low processing requirements to find morphological or stochastic variation neighbourhoods [2, 23].

Machine learning concepts have been efficiently used for detection of abnormal patterns [14, 15] and estimation of brain development [8–10, 17, 22], trauma severity estimation [6, 21] and survival prediction [18, 19, 21], collision avoidance at Heathrow [20], and early detection of bone pathologies [1, 7].

The paper is organized as follows. Section 2 describes the BoSS algorithm in detail. Section 3 describes the experimental setting and results. Section 4 draws practical conclusions from the results and states directions of the research of not yet answered questions.

2 Bag of Synthetic Syllables Algorithm

The algorithm expects the English character set American Standard Code for Information Interchange (ASCII) string of the 1 kB length (though precise Internet message header size is 988 symbols [16]). Any symbol or symbol sequence that does not belong to 'a'-to-'z' or 'A'-to-'Z' intervals is considered as between the words delimiters. Interval 'A'-to-'Z' is converted to the lower case 'a'-to-'z'. Out of the 26 symbols, 6 ('a', 'i', 'u', 'e', 'o', 'y') are considered vowels, and the rest 20—consonants. Synthetic syllables are constructed in the Japanese morae style -2-symbol syllables start with a consonant followed by a vowel. If two vowels follow each other, then two 1-symbol vowel 'syllables' are created. If two consonants follow each other, then one 1-symbol consonant 'syllable' is created.

This synthetic syllabification schema differs from the native English or other languages with alphabetic writing systems texts on which this algorithm may be applied to. For example, the single syllable word 'tree' under this schema will be broken into three synthetic syllables: 't', 're' and 'e'. Such an approach allows keeping controlled compact dimensionality of the feature space and fast mapping into it.

The input short text string then can be represented in the $20 \times 7 + 6 = 146$ dimensional space $\mathcal{S}_{\mathcal{B}\wr\mathcal{SS}} \subset \mathbb{I}^{146} = \text{span}(\mathbf{s}_1 \ldots \mathbf{s}_{146})$, where $\mathbf{s}_i$ is a basis syllable vector. Similarly, it can be interpreted as a 146 bin syllable frequency histogram.

Algorithm 1 The Bag of Synthetic Syllables hash building function

Input: Short text string buffer *str*
Parameters: BoSS hash length $bss\_len = 189$, high (consonant) register lengths $hreg\_len = 27$
Output: BoSS *hash*

```
$memset(hash, \text{‘0’}, bss\_len)$
$str \leftarrow tolower(str)$
$state \leftarrow$ ‘out of syllable’
for all symbols $s_i$, $i \in \{1, \dots |str|\}$ do
    if $state =$ ‘out of syllable’ then
        if $s_i \in \{a, \dots z\}$ then
            if $s_i \in v = \{a, i, u, e, o, y\}$ then
                $hreg \leftarrow j$, where $v_j = s_i$,
                $j \in \{1, \dots 6\}$
                $++hash[hreg * hreg\_len]$
                $state \leftarrow$ ‘out of syllable’
            else
                $lreg \leftarrow s_i -$ ‘$a$’
                $state \leftarrow$ ‘in syllable’
            end if
        end if
    else
        if $s_i \in \{a, \dots z\}$ then
            if $s_i \in v = \{a, i, u, e, o, y\}$ then
                $hreg \leftarrow j$, where $v_j = s_i$
                $++hash[hreg * hreg\_len + lreg]$
                $state \leftarrow$ ‘out of syllable’
            else
                $++hash[lreg]$
                $lreg \leftarrow s_i -$ ‘$a$’
                $state \leftarrow$ ‘in syllable’
            end if
        else
            $++hash[lreg]$
            $state \leftarrow$ ‘out of syllable’
        end if
    end if
    if $state =$ ‘in syllable’ then
        $++hash[lreg]$
    end if
end for
return hash
```

For easiness of computation and visualization (sacrificing a bit of storage space), the short text is also can be represented in the product superspace $\mathcal{S}_{\mathcal{B}\wr\mathcal{SS}} \subset \mathbb{I}^{27} \times \mathbb{I}^{7}$, or a sparse hash of length $27 \times 7 = 189$, where each symbol is calculated as ‘0’ + $n_{\text{syllable occurrences}}$ and a bin location calculated as an offset to ASCII symbol ‘a’ and offset to the set {‘a’, ‘i’, ‘u’, ‘e’, ‘o’, ‘y’} member ‘a’; see Algorithm 1.

When a new short text comes, the lexical and morphological proximity is calculated as a cosine distance $\cos\theta$:

$$\cos\theta = \frac{\mathbf{v}_1 \cdot \mathbf{v}_2}{\|\mathbf{v}_1\|\|\mathbf{v}_2\|} > t_\theta \tag{1}$$

and Euclidean distance d_e:

$$d_\mathrm{e} = \|\mathbf{v}_1 - \mathbf{v}_2\| < t_e \tag{2}$$

and compared to the chosen thresholds t_θ and t_e, where $\mathbf{v}_1$, $\mathbf{v}_2$ are short text vector representations in the $\mathcal{S}_{\mathcal{B}\wr\mathcal{SS}}$ feature space; see Algorithm 2. C code implementation is publicly available at https://github.com/Selitskiy/BoSS.

Example texts: ‘donald: sprucing up for spring’ and ‘vulindlela: sprucing up for spring?’ produce BSS hashes:

‘0001002000 0102030120 0000000000 0000000000 1000000000 0000001000
0000000000 0100000000 0100000000 0000000010 0000000000 0000000000
0000000000 0000000010 1000000000 0000000000 0000000000 0000000000
000000000’

and:

‘0001002000 0003030120 0000000000 0000000010 0000000000 0000001000
0000010000 0100000000 0100000000 0000000010 0010000000 0000000001
0000000000 0000000000 1000000000 0000000000 0000000000 0000000000
000000000’,

with 0.885808 cosine and 2.828427 Euclidean distances.

Algorithm 2 The Bag of Synthetic Syllables hash comparison function

Input: BoSS hashes: h_1, h_2
Parameters: BoSS hash cosine threshold t_θ, Euclidean threshold t_e
Output: BoSS hash proximity flag

```
for all symbols $s_i$, $i \in \{1, \dots |h_1|\}$ do
    $prod \leftarrow prod + (h1_i - \text{‘0’}) \times (h2_i - \text{‘0’})$
    $n2_1 \leftarrow n2_1 + (h1_i - \text{‘0’}) \times (h1_i - \text{‘0’})$
    $n2_2 \leftarrow n2_2 + (h2_i - \text{‘0’}) \times (h2_i - \text{‘0’})$
    $e\_dist2 \leftarrow e\_dist2 + (h1_i - h2_i)^2$
end for
$c\_dist2 = prod^2/(n2_1 \times n2_2)$
if $c\_dist2 > t_\theta^2 \wedge e\_dist2 < t_e^2$ then
    $flag = True$
else
    $flag = False$
end if
return flag
```

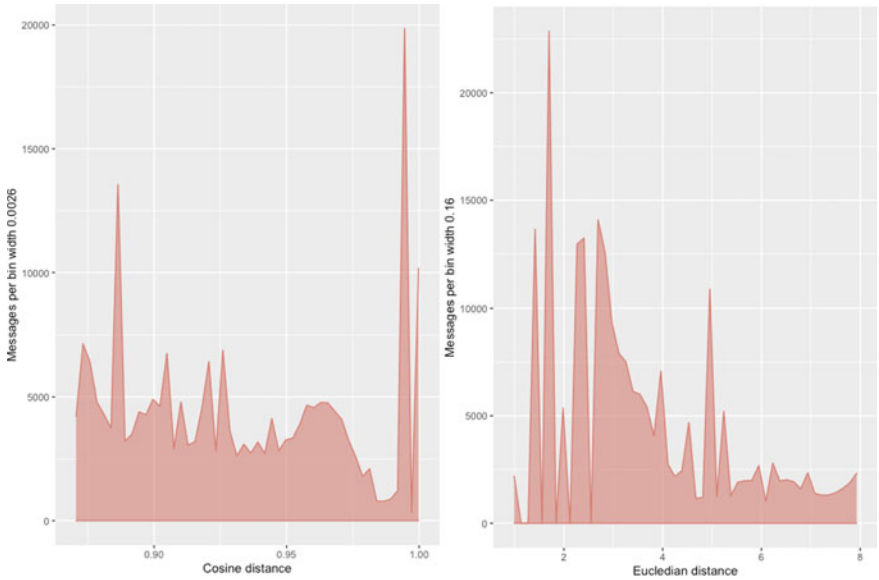


Fig. 2 Cosine (left) and Euclidean (right) distance distribution for messages that triggered BSS proximity verdict. 24 h snapshot

3 Experiments

Experiments were run in the live environment on the Linux Red Hat 7.8 box with 32 GB RAM and Xeon E5-2620 CPU. The BoSS subject header proximity flags were used to generate bulk mail verdicts. Those verdicts, along with the soft SMTP RFC (Request for Comments) standards violations, authenticity verification protocol violations (DKIM [3], SPF [11], DMARC [13], FcRND [4]), associated DNS record malformity, and traffic pattern artefacts verdicts (overall up to 100) were fed into a single perceptron classifier. The classifier performed in the near real-time (4–5 million messages per day, or 0.02 seconds per message processing) and near-zero footprint (additional in-memory buffer of the frequent headers of the size 1000 by 200 bytes line length) mode that does not require any additional hardware or software enhancement of the SMTP server boxes. The classifier was trained in the reinforcement learning style, where each estimate was used as training data for the next time cycle. The training was done in the semi-supervised mode, in which both crowd-sourced labels and few high-fidelity verdicts were used to form the final training label being in the set $\{spam, not\ spam, unknown\}$. Hyper-parameters of the model were set based on the expert estimate and customer feedback, balancing acceptable false positive and false negative error rates. The processing and storage resources constraints put a limitation on the results collected, especially in terms of comparison with other possible algorithms.

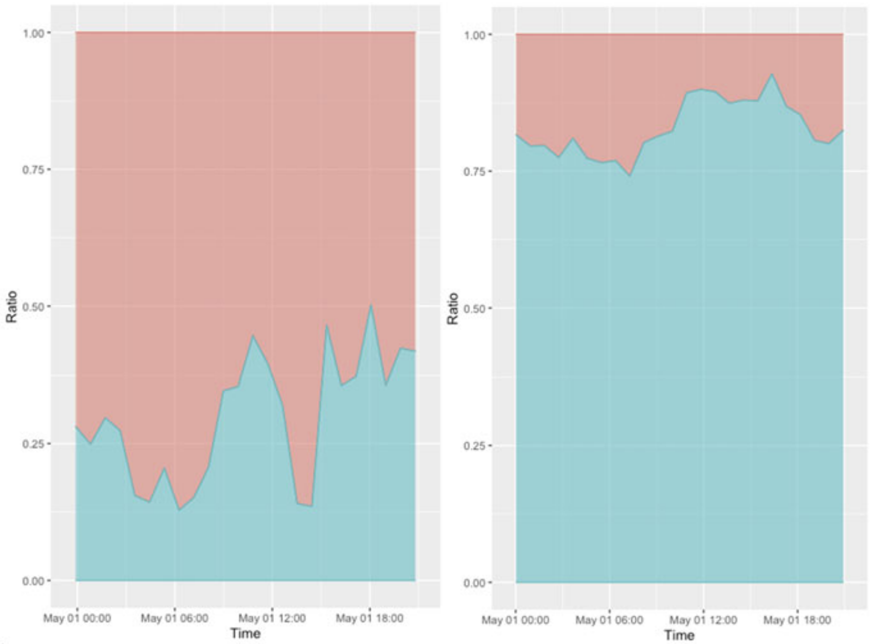


Fig. 3 Proportion of the messages (spam on the left, non-spam on the right) with BoSS spam proximity verdicts (top), and without BoSS spam proximity verdicts (bottom). 24 h snapshot

Based on the one-day traffic, it can be seen that majority (again circa 90%) of the bulk mail subject lines is not varying (2,161,679), while 216,877 messages have intentionally or unintentionally mutated subject lines with cosine distance in (0.87–1.00) interval, which was used as a criterion of the subject line variational and morphological proximity for the cosine distance distribution and Fig. 2 for the Euclidean distance distribution. The threshold cosine distance 0.87 was selected from ±0.05 interval based on the expert estimate and customer feedback.

BoSS proximity verdict associated with particular IP ranges, sender domains and other source information do not necessarily mean that the messages coming from these sources are spammy but rather indicate the incoming stream's bulk nature. The bulk mail can be either genuine reporting such as retail or bank statements or social media or subscription notifications that some users may desire and are better to be categorized as grey mail Fig. 4.

Therefore, BoSS proximity verdicts are meant to be used with other mentioned above verdicts as input for machine learning (ML) algorithms, preferably fast and effective shallow solutions that can utilize the lightweight BoSS approach. Nevertheless, the association of the BoSS proximity verdict with spam verdicts can be seen on Fig. 3.

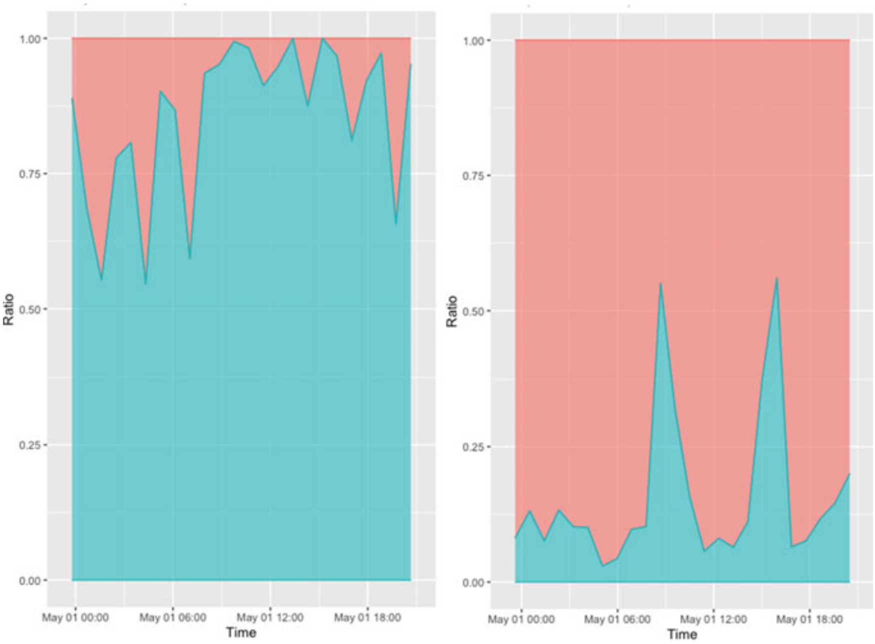


Fig. 4 Proportion of the messages (from banks on the left, social on the right) with BoSS spam proximity verdicts, and without BoSS spam proximity verdicts (bottom). 24 h snapshot

4 Discussion and Future Work

Bag of synthetic syllables algorithm offers a less dimensional space than typical bag of words algorithms. However, the BoSS algorithm still has enough discriminating power to strongly associate its verdicts with bulk spam or grey mail. Economical, near zero-footprint use of hardware resources and fast near real-time operation allows it to be used as the first line of defence, unloading more sophisticating but slow and resource-demanding DL algorithms.

For future work, a multi-perceptron ML layer working with BoSS verdicts as inputs can distinguish the bad spam verdicts from various flavours of the grey bulk verdicts.

References

1. Akter M, Jakaite L (2019) Extraction of texture features from X-ray images: case of osteoarthritis detection. In: Yang XS, Sherratt S, Dey N, Joshi A (eds) Third international congress on information and communication technology. Springer, pp 143–150
2. Bojanowski P, Grave E, Joulin A, Mikolov T (2016) Enriching word vectors with subword information. CoRR abs/1607.04606

3. Hansen T, Kucherawy M, Crocker D (2011) DomainKeys identified mail (DKIM) signatures. https://tools.ietf.org/html/rfc6376. Accessed 31 Jan 2021
4. Howard L (2018) Reverse DNS in IPv6 for internet service providers. https://tools.ietf.org/html/rfc8501. Accessed 31 Jan 2021
5. Jain G, Sharma M, Agarwal B (2019) Int J Inf Technol. Optimizing semantic LSTM for spam detection 11(2):239–250
6. Jakaite L, Schetinin V (2008) Feature selection for Bayesian evaluation of trauma death risk. In: 14th Nordic-Baltic conference on biomedical engineering and medical physics: NBC 2008 Riga. Latvia. Springer, Berlin, Heidelberg, pp 123–126
7. Jakaite L, Schetinin, V, Hladuvka, J., Minaev, S., Ambia, A., Krzanowski W (2021) Deep learning for early detection of pathological changes in X-ray bone microstructures: case of osteoarthritis. Sci Rep 11
8. Jakaite L, Schetinin V, Maple C (2012) Bayesian assessment of newborn brain maturity from two-channel sleep electroencephalograms. Comput Mat Methods Med 1–7
9. Jakaite L, Schetinin V, Maple C, Schult J (2010) Bayesian decision trees for EEG assessment of newborn brain maturity. In: The 10th Annual workshop on computational intelligence
10. Jakaite L, Schetinin V, Schult J (2011) Feature extraction from electroencephalograms for Bayesian assessment of newborn brain maturity. In: 24th International symposium on computer-based medical systems (CBMS). Bristol pp 1–6
11. Kitterman S (2014) Sender policy framework (SPF) for authorizing use of domains in email, version 1. https://tools.ietf.org/html/rfc7208. Accessed 31 Jan 2021
12. Klensin JC (2008) Simple mail transfer protocol. https://tools.ietf.org/html/rfc5321. Accessed 30 Jan 2021
13. Kucherawy M, Zwicky E (2015) Domain-based message authentication, reporting, and conformance (DMARC). https://tools.ietf.org/html/rfc7489. Accessed 31 Jan 2021
14. Nyah N, Jakaite L, Schetinin V, Sant P, Aggoun A (2016) Evolving polynomial neural networks for detecting abnormal patterns. In: 2016 IEEE 8th International conference on intelligent systems. pp 74–80
15. Nyah N, Jakaite L, Schetinin V, Sant P, Aggoun A (2016) Learning polynomial neural networks of a near-optimal connectivity for detecting abnormal patterns in biometric data. In: 2016 SAI computing conference. pp 409–413
16. Resnick PW (2008) Internet message format. https://tools.ietf.org/html/rfc5322. Accessed 30 Jan 2021
17. Schetinin V, Jakaite L (2012) Expert Syst Appl. Classification of newborn EEG maturity with Bayesian averaging over decision trees 39(10):9340–9347
18. Schetinin V, Jakaite L, Krzanowski W (2018) Int J Med Inf. Bayesian averaging over decision tree models: an application for estimating uncertainty in trauma severity scoring 112:6–14
19. Schetinin V, Jakaite L, Krzanowski W (2018) Artif Intell Med. Bayesian averaging over decision tree models for trauma severity scoring 84:139–145
20. Schetinin V, Jakaite L, Krzanowski W (2018) Integ Comput-Aided Eng. Bayesian learning of models for estimating uncertainty in alert systems: application to air traffic conflict avoidance 26:1–17
21. Schetinin V, Jakaite L, Krzanowski WJ (2013) Expert Syst Appl. Prediction of survival probabilities with Bayesian decision trees 40(14):5466–5476
22. Schetinin V, Jakaite L, Schult J (2011) Informativeness of sleep cycle features in Bayesian assessment of newborn electroencephalographic maturation. In: 24th International symposium on computer-based medical systems, pp 1–6
23. Sureka A, Jalote P (2010) Detecting duplicate bug report using character n-gram-based features. In: 2010 Asia Pacific software engineering conference, pp 366–374
24. Wu T, Liu S. Zhang J, Xiang Y (2017) Twitter spam detection based on deep learning. In: Proceedings of the Australasian computer science week multiconference. ACSW'17. Association for Computing Machinery, New York, NY, USA
25. Zhang Y, Jin R, Zhou ZH (2010) Int J Mach Learn Cybern. Understanding bag-of-words model: a statistical framework 1(1):43–52

An Approach for Learning Polish Braille Mathematical Notation by Sighted Teachers Based on Liblouis Converters

Dariusz Mikulowski

Abstract Teaching mathematics to blind students is not an easy task. To read and write formulas, the blind students use the Braille alphabet and special Braille mathematical notations that are different forms in different countries. Such notation encodes mathematical symbols and whole structure of the formula in the form of Braille point signs. Teachers in mainstream schools usually encounter various problems while teaching the blind to math. One of these difficulties is their lack of knowledge of the Braille alphabet and, in particular, of Braille mathematical notation. To facilitate their cooperation with blind students, we propose a solution by which these teachers can learn the basics of Polish Braille mathematical notation (in short, BNM). It was implemented as a web application and tested by four sighted users. The application received positive feedback, although a solution must be improved and more deeply tested.

Keywords Teaching math · Braille mathematical notation · Blind students · Math teachers

1 Introduction

Learning maths is very problematic for visually impaired and blind students (BVI) for several reasons. They face significant barriers in accessing mathematical literature because they can not use the standard alphabet of the sighted people. Instead, they use the Braille alphabet [1] with a unique code for mathematic formulas called Braille math notation. For these reasons, reading and writing mathematical formulas by the BVI is much slower than in the case of sighted individuals.

Another problem is the insufficient preparation of teachers who works with BVI students. While in schools dedicated to the blind, math teachers are well-prepared

D. Mikulowski (✉)
Faculty of Exact and Natural Sciences, Siedlce University of Natural Sciences and Humanities, Siedlce, Poland
e-mail: dariusz.mikulowski@uph.edu.pl

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_23

because they also know Braille's mathematical notation. In mainstream schools, the situation is much worse. According to research carried out in the frame of the Euromath project [2], it turns out that about 48 percent of math BVI teachers from mainstream schools in Poland, Ireland and the Netherlands do not know Braille and even Braille mathematical notation. Therefore, there is a great need to support them in teaching mathematics they lead.

In this paper, we propose a solution that may be a step toward solving this problem. It uses open-source converters extending the Liblouis library [3] to teach Polish Braille math notation (BNM) [4] to sighted teachers and tutors.

The structure of the rest of this paper is as follows:

- In the next section, we will present the problem of many mathematical Braille notations in different countries and the differences in the writing of formulas by sighted and blind people. We will also present the existing solutions supporting the writing and reading of formulas by the blind.
- In the next section, we will introduce a bit more about Liblouis-based converters and present how our solution works.
- In the result section, we will describe how we have verified our solution.
- Then, in conclusion, we will give a summary of our research and plans for future work.

2 Braille Mathematical Notations and Solutions

2.1 Braille Mathematical Notations

The Braille alphabet was invented in 1824 by the brilliant blind student of the Paris school for the blind, Louis Braille [1]. As a part of his alphabet, he also developed the original versions of mathematical and musical notations. However, in the following years, the differences in the blunt development of the education of the blind in all countries and the different conditions that prevailed in them developed many mathematical notations are sometimes very different from each other [5]. As a result, the mathematical notation created in one country is incomprehensible to the blind living in another one. This is turning out to be a big problem.

Blind people in most US states use a notation called Nemeth-Code [6]. The name Nemeth-Code comes from its author's name, Dr Abraham Nemeth. It was established in 1946 and adopted as a standard by the Braille Authority of North America (BANA) in 1952. Then it has been developed ever since. Dr Nemeth intended to make it possible to write down formulas dealing with complicated problems of different math branches such as algebra, geometry and even differential calculus or integrals. A characteristic feature of this notation is that the math expression takes up a relatively large amount of space compared to other solutions. The author's idea was to create a writing system that would be as similar as possible to that of the sighted.

Another example of math Braille notation is the German notation known as Marburg [7]. It was created by Helmut Epheser, Karl Britz and Frideruch Mittelsten Scheid at the Marburg School for the Blind in 1955. This system is used in German-speaking countries and few other places. In the following years, it has undergone several modifications and its last update was released in 1992. Polish Braille mathematical notation (BNM), used in the research described in this article, was also created based on Marburg system.

Another example of mathematical Braille notation is the English notation called Unified English Braille (UEB) [8]. Its development was aimed at standardizing several systems used in these countries so that blind people would not have to use several different Braille codes. The idea behind this notation was to create a code that combines three official Braille notations: literary material (English Braille), mathematical notation (NemethCode) and computer notation (Computer Braille Code). In 1993, this project was adopted by the International Council on English Braille (ICEB). The originators of this unification were Dr T. V. Cranmer and Dr A. Nemeth. The intention was to create a code similar to the literary Braille used in all English-speaking countries.

In addition to the notations mentioned above, other countries have their own Braille mathematical notation systems. Spanish-speaking countries have their notation, the Czechs have developed their system, and the Russian-speaking countries have also their notation.

As we mentioned above, Polish BNM notation [4] was based on the Marburg notation. It was developed in 2002 by a consortium of all mathematics teachers from schools for the blind in the country. Its latest version was published in 2011. This notation, apart from a set of mathematical symbols, also includes symbols needed to write physical dependencies and chemical formulas.

To better explain the essence of differences in these notations, we summarize this section with a small demonstrative. For example, it will illustrate different approaches to present formulas in different Braille mathematical notations, and we will show the expression of the same mathematical formula in the Nemeth-Code and BNM. Let us take the following formula:

$$\frac{\frac{1}{2}+\frac{1}{3}}{6}$$

Its expression in the Nemeth-Code notation is shown in Fig. 1.

In turn, the same formula in the Polish mathematical notation is shown in Fig. 2.

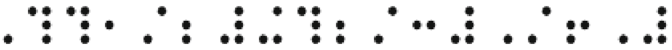


Fig. 1 Formula in Nemeth-Code

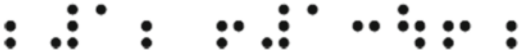


Fig. 2 Formula in Polish Braille math notation

As we can note, the differences in the concepts of both notations are significant. There are symbols in each notation, i.e. the beginning of the expression, the end of the expression, the fraction bar and others. However, they have a different arrangement of Braille points. We can notice that in the Polish notation based on Marburg, the brevity of the notation is emphasized, which means that certain symbols may be omitted in some contexts. On the other hand, Nemeth-Code was supposed to be a notation similar to the notation of sighted people. Therefore, the formula is written in it with more characters. It is also easier to process automatically because each part of the formula has a tagged beginning and end, and the occurrence of symbols does not depend on their context.

Such a state of affairs means that Braille notation converters are needed to support mathematics teaching using a computer. Moreover, they are necessary to transform the notation of sighted people into Braille notation and vice versa. One of the most popular converters is the Liblouis library used in our research. We will describe it in the next section.

2.2 *The Liblouis Converters*

Liblouis is an openly licensed universal converter that converts various mathematical notations into Braille and vice versa [9]. It has been implemented as a C++ library and a set of tables and semantic files. They are then used for semantic replacement of the symbol sequences from one notation with another. It allows for automatic translation of mathematics from standards such as MathML [10] and LaTeX [11] into Braille notation. Thanks to Liblouis, the reverse translation is also possible. The Braille mathematical formulas can be translated into MathML or Latex. Liblouis can be adapted to any Braille notation by creating an appropriate set of tables and configuration files and implementing the library's missing functions if needed. Such adaptation to the use of Polish Braille mathematical notation was made as part of the PlatMat project [12]. It was also used in the research we are describing in this paper.

The converter works by running the translation (MathML Braille) or back-translation (Braille MathML) function. It takes the name of the configuration file for the given Braille notation and the names of the input and output files as arguments. In turn, in the configuration file, there are references to various tables and semantic files. In these tables, the characters from the input and the corresponding sequences of characters that should be written to output are encoded. In addition, there are semantic rules that determine in what contexts and in which course the input sequence is to be converted into an output sequence. The conversion is performed in three following steps.

- In the first step, the input data is initially processed to output. At this stage, some document elements that will be processed in the following stages are appropriately tagged.

- The second pass processes the document more thoroughly. The places that were marked in the first run are replaced with the appropriate output sign sequences. At this stage, for example, math formulas are processed using semantic rules.
- The last pass is called the edit pass. In this step, final corrections of the output format are made, such as adding spaces before the math operators or adding Braille page numbering, etc.

To summarize this section, we will give an example of converting a formula from MathML format to Polish Braille mathematical notation. Let take the formula we presented in the previous section, namely

$$\frac{\frac{1}{2}+\frac{1}{3}}{6}$$

Its MathML representation is as follows:

```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<math xmlns="http://www.w3.org/1998/Math/MathML">
  <mfrac>
    <mrow>
      <mfrac>
        <mn>1</mn> <mn>2</mn>
      </mfrac>
      <mo>+</mo>
      <mfrac>
        <mn>1</mn> <mn>3</mn>
      </mfrac>
    </mrow>
    <mrow>
      <mn>6</mn>
    </mrow>
  </mfrac>
</math>
```

After performing the conversion from this MathML code, we will get the appropriate ASCII string that denotes the Braille formula. It will be the following string.

```
;#a; +#a: 8+
```

where sign `;` (semicolon) means the beginning of the main fraction, `#a;` means small fraction (`#a` means 1 in the numerator) and `;` means 2 in the denominator In addition, signs `#a:` means small fraction $\frac{1}{3}$ and `8` means the fraction bar of the main fraction and < means end of the whole fraction.

As we can note, even from this simple example, coding maths formulas in Braille is not a trivial thing. After changing the font of the above formula representation sequence to Braille or sending this text to a Braille printer [13, 14], we will get the appropriate pattern of points as shown in the formula presented in Fig. 2. Using Liblouis, there is also possible the conversion in the opposite direction. The ASCII string denoting a Braille formula can be performed to the appropriate MathML fragment.

The Liblouis library is currently used in many programs supporting the work of the blind, such as screen readers and software for creating Braille publications, and even in such solutions as software Braille keyboards for mobile phones.

2.3 Tools Supporting Learning Math by BVI

Considering the difficulty of learning mathematics by BVI, several tools have long been developed to make it easier for them. As the first teaching aids for learning mathematics for BVI, there were simple manual tools such as Nicholas Saunderson's algebraic board, William Taylor's octagonal plate, or Christian Meyer's calculator [15]. With the advancement of technology, new opportunities have emerged. There were developed special software that would allow the printing of Braille textbooks containing mathematical content. These were applications such as Winbraille [16] or Duxburry [3, 17]. Braille, Brailkom and Euler applications have been developed in Poland [18].

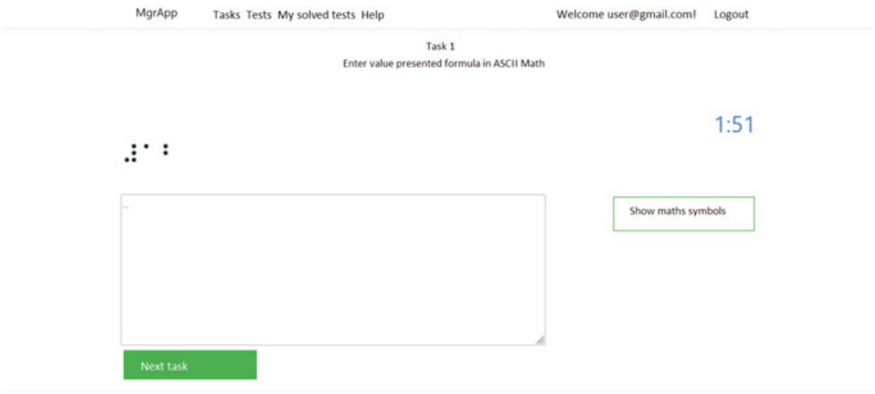
Along with web technologies and applications, new solutions appeared that allow learning mathematics using a web browser. These are such systems as Desmos [19] or Euromath [12]. To a limited extent, BVI can also use the equation editor in MS Word. There is also a special plugin for the NVDA screenreader [20] that translates the Latex representation to text form. Then this text representation may be spoken by the voice of the speech synthesizer [21].

However, to the author's knowledge, no solution would allow mainstream schools teachers to quickly and comfortably learn mathematical notation. As a step toward solving this problem, we propose an application for learning Polish Braille mathematical notation, which we will present briefly in the next section.

3 How It Works

As an implementation of the proposed solution, a pilot web application has been developed. It allows learning BNM notation by sighted users (teachers, parents and tutors of blind students).

There are two types of users of our application: student and administrator The administrator can manage tasks, add, delete and edit tasks and put them in the appropriate math branch sections. We used the publication untitled Polish Braille math-


Task 1

Enter value presented formula in ASCII Math

Fig. 3 Solving the task in web learning application

ematical physical and chemical notation [4] as the substantive content to fill the application with tasks.

The second type of user is the student. He can solve problems by writing formulas of different branches of mathematics. These tasks can be divided into two main types: Braille writing tasks and Braille reading tasks. Solving the Braille reading task is that the application displays an exemplary formula in the Braille points, as the blind save it in BNM. The user then writes this formula in the well-known AsciiMath notation. If the formula was written correctly, it is graphically displayed thanks to its previous conversion from AsciiMath to MathML. The writing tasks are the reverse process. First, the application displays the formula in a graphical form, and stores in MathML in the user interface, and the user is asked to write the formula in Braille. Typing involves using the f d s j k l keys from the regular qwerty keyboard, pressed sequentially. These keys represent Braille dots from 1 to 6, respectively. After entering the whole character, e.g. in the case of the letter b, pressing the Braille dots 1 and 2, i.e. the f d keys, the user presses the separation key h. In this way, he thus completes the entered Braille character. By continuing this process, the user can write down the whole formula. When the task is completed, the formula is displayed in two forms, i.e. in graphical and Braille form, and the user is informed about the correct solution of the task. The application also has a test mode in which the user has 2 minutes to solve each task. Figure 3 shows the process of solving the test by a user.

The administrator can perform all usual activities on tasks and math branch sections gathered in the application. He can add, delete, publish and remove them from publication. Figure 4 shows the screen that allows adding a new task to the application.

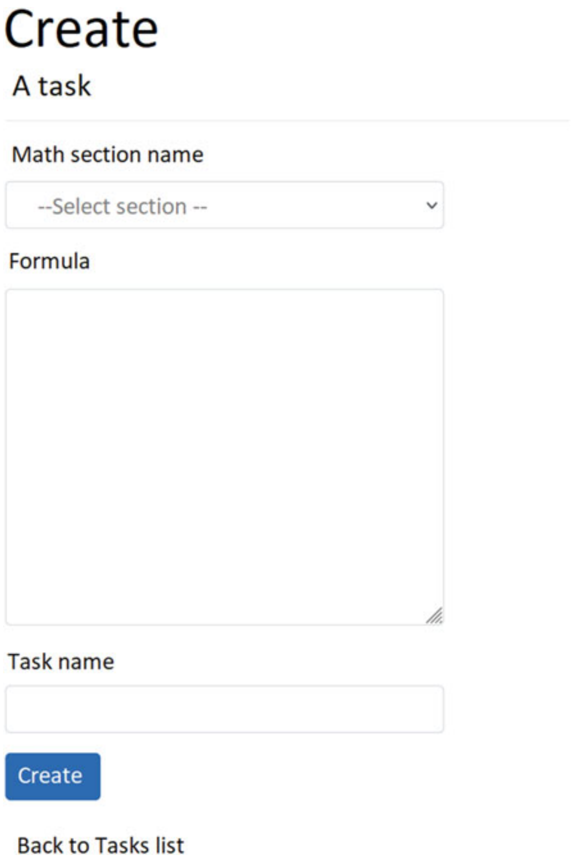


Fig. 4 Adding a task to the learning application

4 Verification of Our Solution

The web application has been pre-verified by future users. We invited four sighted testers to evaluate our application. The application was filled with 38 tasks and two tests. The testers were to register in the system, solve as many tasks as possible and solve the created tests. After completing solving tasks, users were asked to comment on the intuitiveness of the UI and the data input mechanisms used in the application. The testers were to express their satisfaction with the application and the method of entering the formulas on a scale of 1–4: 1 not satisfied, 2—somewhat satisfied, 3—satisfied and 4—very satisfied. The investigation results are presented in Table 1.

After completing the tasks, all testers found that they could learn something new in a relatively pleasant and straightforward way. They recognized that the application has potential power, and the interface is clear and legible. They also confirmed that the proposed manner of solving tasks is pleasant although it requires few minutes of prior training.

Table 1 Results of testing a training application by users

	User 1	User 2	User 3	User 4
Number of solved tasks	38	38	30	22
Number of solved tests	2	2	2	1
Satisfaction with the app	4	4	2	2
Satisfaction with the method of entering formulas	4	4	3	3

5 Conclusions and Future Works

In the paper, we proposed a solution that allows sighted users to learn Polish Braille mathematical notation. It was implemented in the form of a prototype application and verified by four sighted users. They expressed their satisfaction with using it. We are planning to test the application among a more significant number of users. The application can be adapted to the needs of the blind so that also blind beginners could use it. In addition, the use of the universal Liblouis converter makes it possible to adapt the solution to other Braille mathematical notations such as UEB or Marburg. Thanks to this, the solution will also be helpful for teachers in other countries.

References

1. Kamei-Hannan C, Sacks S-Z (2012) J Vis Impair Blind. Parents perspectives on Braille literacy: results from the ABC Braille study 106(4):212–223
2. Brzostek-Pawlowska, J, Rubin M. Mikulowski D (2019) Technologie informacyjno-komunikacyjne zwiększające dostępność treści matematycznych. in: Adam Marszałek. Toruń
3. Zatserkovnyi R, Mayik V, Zatserkovna R, Mayik L (2019) Analysis of Braille translation software. Printing Publish 2:36–44. https://doi.org/10.32403/0554-4866-2019-2-78-36-44
4. Budzanowska K, Broniarz K, et al (2011) Brajlowska notacja matematyczna, fizyczna i chemiczna. Edition II, 2011. Polish Association of the Blind Warszawa
5. World Braille usage, 3rd edn. UNESCO, 2013. https://www.perkins.org/assets/downloads/worldbrailleusage/world-braille-usage-third-edition.pdf. Accessed 12 2018
6. Interview with Dr. Abraham Nemeth. https://nfb.org/images/nfb/publications/fr/fr28/fr280110.htm. Accessed July 2021
7. Nikisha J, Bankim P (2016) Transliteration of digital Gujarati mathematical text into Braille for visually impaired people. Int J Latest Trends Eng Technol (IJLTET) 7:217–229. https://doi.org/10.21172/1.73.531
8. Andrea D (2013) Unified English Braille: the future of Braille in the United States. J Vis impair Blind 107:243–246. https://doi.org/10.1177/0145482X1310700311.2013
9. Liblouis.org. (2021) Liblouis—An open-source braille translator and back-translator. http://liblouis.org/. Accessed Sept 2021
10. Wright F (2000) Interactive mathematics via the web using MathML. In: ACM Sigsam Bull 34. https://doi.org/10.1145/362001.362022
11. Sufian A (2019) Article writing using LaTeX. https://doi.org/10.13140/RG.2.2.26707.43043

12. Mikulowski D, Brzostek-Pawlowska J (2020) Multi-sensual augmented reality in interactive accessible math tutoring system for flipped classroom. in: Intelligent tutoring systems. Springer, pp 1–10. https://doi.org/10.1007/978-3-030-49663-0-1
13. Take a look at a selection of Viewplus braille printers. ViewPlus. https://viewplus.com/braille-printers/. Accessed 05 Apr 2018
14. Braille printers/Braille embossers by index Braille—Index. 2021 Index Braille https://www.indexbraille.com/. Accessed Oct 2021
15. Ptak JF (2021) 18th Century calculator for the Blind–Nicholas Saunderson, Mathematician. https://longstreet.typepad.com/thesciencebookstore/2008/05/18th-century-ca.html. Accessed June 2021
16. Blomquist M (2002) Braille contractions in WinBraille. In: Miesenberger K, Klaus J, Zagler W (eds) In: International conference on computers for handicapped persons ICCHP 2002: computers helping people with special needs, vol 2398. Springer, Berlin, Heidelberg, pp 602–609. https://doi.org/10.1007/3-540-45491-8-117
17. Nadeem M, Aziz N, Sajjad U, Aziz F, Shaikh H (2016) Comparative analysis of Braille generation technologies, pp 294–299. https://doi.org/10.1109/ICARM.2016.7606935
18. Euler-Braille translation software. Index Braille. https://www.indexbraille.com/en-us/support/braille-editors/euler. Accessed 09 2021
19. Inc. Desmos: Desmos graph. https://www.desmos.com/calculator. Accessed 18 Apr 2018
20. NV access: empowering lives through non-visual access to technology. 2021 NV Access Limited. https://www.nvaccess.org/. Accessed 09 2021
21. Ahmetovic D, et al (2018) Axessibility: a LaTeX package for mathematical formulae accessibility in PDF documents. in: Proceedings of the 20th international ACM SIGACCESS conference on computers and accessibility, pp 352–354

Low Energy Response of Spike Train Encoded Data

Carrie Hartley Segal

Abstract A low energy response of data encoded from a single time representation into a temporal spike train results in a sparse non-binary digital code useful for instantaneous or near-instantaneous communication of select messages. When an integrated circuit senses, an analog signal is typically converted to binary digital information. Instead, we create Markov chain data generator circuits to produce temporal spike trains which are non-binary digital signals with varying degrees of ergodicity or non-ergodic. We build a software emulator of a hardware non-binary digital circuit to demonstrate efficient data transfer of information as a non-binary digital signal. We demonstrate data reduction on streaming digital video and emulate the hardware design of an analog to non-binary digital circuit implementation. The ergodic non-binary digital signals achieve 100× data reduction over conventional binary data.

Keywords VLSI · Markov chain · Spiking neural network · Low energy · Data compression

1 Introduction

Noiseless digital circuit design is predominantly implemented using static complementary metal oxide semiconductor (CMOS) fabrication [18]. Boolean logic gates are designed into standard cells with static timing parameters for specific fabrication processes, which have statistically predictable behavior from intensive simulation, fabrication, measurement, repeated multiple times. The intensive analysis means the standard cells are taken as a 'gold standard' of the operating parameters for a specific process technology node (denoted by the minimum feature length available in that process, i.e., 500, 130 or 12 nm. (*Processes range from large feature sizes* $1um$ *micron through recent processes down to* $2nm$.)

C. H. Segal (✉)
University of California, Santa Barbara, Santa Barbara, CA, USA
e-mail: chsegal@ece.ucsb.edu

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_24

A binary digital circuit is built using automated tools to first translate a register transfer level (RTL) design into an assorted collection of combinational logic assuming static time and using only the cells available in that process. Then, the design will undergo timing analysis and have additional supporting cells added, such as buffer's to speed up signals which need to travel a long distance. Next, sequential logic is added to interconnect the combinational logic blocks and the entire design is checked for timing to make sure that propagation delays from one area of the circuit will not impact logic further downstream. Using this manner of design translation from RTL to physical design results in a final design where the power used to transfer a signal is disconnected from the signal information.

It is beneficial to support a disconnect between function and physical implementation, but as RTL designs grow in complexity, there is a point where the circuit is no longer able to meet static timing requirements, and the formerly noiseless digital signals are prone to upset and timing errors. The only solution to a physically large design that is unable to meet the timing requirements is re-design, a costly process generally avoided. Neuromorphic integrated circuit design has these difficulties because the designs are often mixed-signal designs with substantial portions of the overall area dedicated to digital logic.

An alternative to this is to embrace alternate design styles which are intrinsically connected to the physical characteristics of the process they are implemented in. Equilibrium propagation, which equates the Kirchoff model of a circuit to the operation of a neural cell, is able to signal a response based on the overall inference of the network as it finds a energy minimum to settle around for a learned pattern [23]. End-to-end training implementations using equilibrium propagation are aware of the power hungry effects of analog-to-digital and digital-to-analog conversion, and propose an energy efficient system which minimizes those components in circuit implementations [10].

Previous work on sparse coding strategies have demonstrated their high capacity at storing representations within small networks. [3] Neuromorphic hardware is able to efficiently process sparse codes leading to highly efficient computation. [31] Artificial intelligence datasets, used for training and benchmarking computational models, are often provided in digital form and need converted back to an analog signal that is intended to be received by a neuromorphic sensor for proper studies of how functional a hardware algorithm could be [8]. Communication from an integrated circuit sensor, like a dynamic vision sensor [11] or other neuromorphic sensor [17], use address-event representation (AER) to communicate that an event occurs at a specific address on the read-in sensor [1]. AER produces an itemized listen of channel identities and timestamps of when events occurred [32]. Often converting the dataset into AER is acceptable to perform behavioral studies. [6]

In some circumstances, reconstruction of the sensor data based on the digital data in a dataset is necessary to create data for the specific experiment. In this work, an address-event representation of data is created based on a predetermined Markov chain. The reason for doing so is to study the effects of how an analog sensor could encode a AER version of the image to be transmitted and decoded. These predetermined Markov chains are used to construct a two-dimensional circuit which transmits a simplified yet data-rich stream of video and sensor information. This AER stream is useful to quickly decode an information-rich scene from a vision sensor. A prototype of how this system operates is demonstrated on the streaming video of a computer camera. Additional experiments look at the Berkeley Driving dataset, while converted into AER format. While any data can be converted into AER it may be impractical to keep data in that format because in the worst case, an address and event time must be stored for every bit in every pixel of the sensor. A way to mediate that dilemma is to directly convert the data into a non-binary digital temporal spike train at the sensor readout.

2 Preliminaries

The information content of a message is described using Shannon entropy H, a term which measures how much information is produced at some rate from an information source with symbols present with probability $P = \sum_{i=1}^{n} p_i = 1$.

$$H = -A_\chi \sum_{i=1}^{n} p_i \log_n p_i \tag{1}$$

The way the overall probability P is distributed across the symbols from the alphabet determines the classification of Markov chain the message could come from [2]. The original applications of entropy to electronic communication were pioneered by Bell Labs through the work of scientists [24] [7], and [19]. Continued development on the applications and uses of entropy estimation have continued through to the present day. Digital data compression benefits from Shannon's noiseless coding theorem to deliver compression at the Shannon limit for binary data [12]. Raptor codes for error correction allow for full data recovery from a datastream after $k(1+\epsilon)$ symbols are received [25].

Shannon entropy for continuous vs discrete takes the unit of measure for a continuous signal as A_χ [24]. For a discrete signal, the unit of measure is equal to the symbols used to discretize the continuous signal and is a constant A_χ. [12] With analog signals, an electrical communication is a continuous function $V(t)$; when the conversion is made from analog-to-digital, the selection of A_χ is performed [22].

Beginning with binary means the data is already discretized and the value of $A_{\text{binary}} = 2$ because there are two symbols in a binary alphabet [21]. That is also dependent on any additional encodings which would only increase A_χ that takes place over time T. Those additional encodings are dependent on previously communicated symbols, and these encoding will be limited to less than a signal converted from analog-to-digital with a naturally higher A_χ. With a known Markov chain, we can estimate the entropy using an estimator [9] and compare against the known entropy of the Markov chain.

2.1 Race Logic Circuits for Non-binary Digital Codes

Alternative computing based on temporal ‘race’ logic enables non-binary encoding [28]. The state identity of a symbol can be encoded based on the transit of a single solitary wire [13]. A system using two-wire ($w = 2$) encoding to indicate ‘1’ with a wire and ‘0’ with the other wire is used for high-speed signaling in asynchronous circuits [16]. Systems with $w > 2$ are theoretically proven and physically simulated to solve classification problems [27].

Race logic is a CMOS implementation of Boolean logic that embeds the timing and data information into a single edge or pulse. [13] A compute grid of identical cells is configured with a 1D program broadcast across an array with the unit cells providing alternative timing paths dependent upon the ‘program’ stored in the stationary computation vectors R and Q [14].[1] Each of the individual compute elements operates on stationary binary input signals, and the communication signal which propagates out the end point of the circuit is a non-binary signal which decodes to the result of the program.

CMOS circuits to implement race logic are concerned with the measurement of a transition $\overline{01}$ [26]. The physical measurement has transition probability equivalent to a first-order binary Markov source.

$$P_{\text{FOBMS}} = \begin{bmatrix} p_{0|0} & p_{0|1} \\ p_{1|0} & p_{11} \end{bmatrix} \tag{2}$$

For the binary source, the stationary probability vector is represented as $(\mu(0), \mu(1))$, where

$$\mu(0) = \frac{p_{0|1}}{p_{0|1} + p_{1|0}}, \mu(1) = \frac{p_{1|0}}{p_{0|1} + p_{1|0}} \tag{3}$$

The reset state is taken from the two binary options. It is the state corresponding to the stationary distribution $p(\chi_1 = 0) = \mu(0)$, or the probability that if the reset state is 0, the probability of observing $\mu(0)$ is 1. From reset, χ^n represents all possible n-bit sequences containing a single transition as a second order Markov chain from the original first-order stationary distribution with reset. That sequence $z_1 = 0^{n-\ell}1^{\ell}$ has a sequence of $n - \ell$ 0’s followed by ℓ 1’s. ([5])

An entropy estimation taken by sampling the output wires would need to gather independent samples at multiple times, equal to the number of possible symbols (2 for `binary`), before it would be able to return accurate estimates. ([9])

A first-order non-binary Markov source, that is, *simply ergodic* is one that has at minimum a non-zero probability of transition in each row. Furthermore, to establish a baseline entropy to energy equivalence, a first-order Markov source has a *B-system ergodic* if for each $p \in P_\chi = 1/\chi^2$

[1] The references on race logic use P and Q . In this work, R is used instead of P to prevent confusion with P probability.

$$P_{\text{FONBMS}} = \begin{bmatrix} p_{00} & p_{01} & \cdots & \cdots \\ p_{10} & p_{11} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & p_{A_\chi == H_\chi} \end{bmatrix} \tag{4}$$

If the number of symbols is increased from binary to 3 or greater symbols, as demonstrated in Fig. 1, where 3 symbols, `fast` , `medium`, and `slow` are shown as voltage timing waveforms, the entropy cost to access the reset state increases with the entropy of the order of the Markov chain $\frac{1}{2}\log n$. Where n is the number of possible symbols used by the specific implementation of the non-binary digital encoding.

The increasing entropy penalty with code length n means that for a physical implementation of a unit cell, the energy cost to reset should grow quickly at first with the number of unit cells. However, as the number of unit cells increases toward larger magnitudes, the energy cost to reset the unit cells should not differ significantly. Figure 2 demonstrates the theoretical cost of reset that is acceptable for a race logic circuit. The solution for our circuit, to achieve closer to theoretical reset, is to move from a 1D Race logic circuit to a 2D design based upon an original known 1D race.

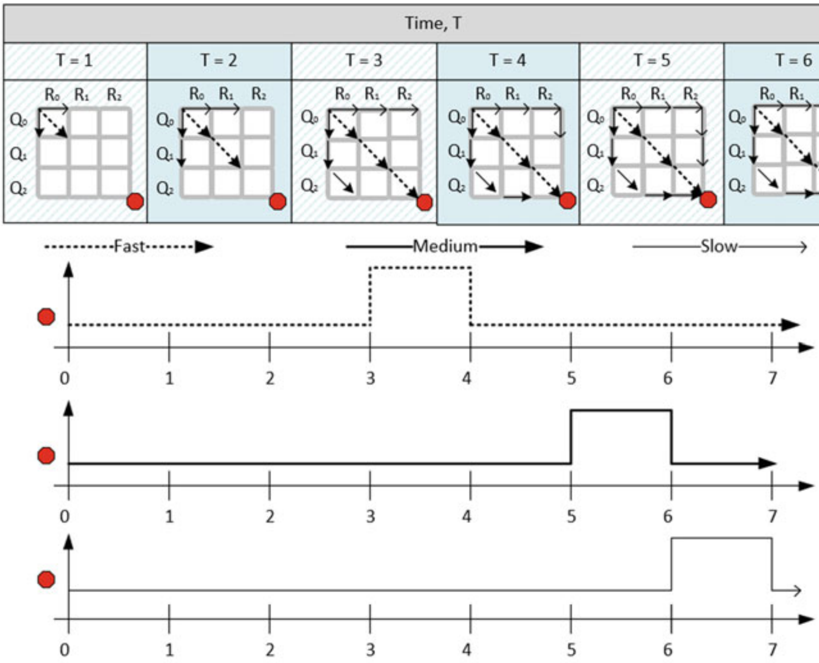


Fig. 1 Racelogic circuit with $A = 3$ symbols, **fast**, **medium**, **slow**, shown as voltage timing waveforms. A 1D compute grid operated on stationary program signals Q and R to configure the timing path of an incoming spike (upper left corner) which eventually leaves the 'race' (octagon, lower right corner) encoded with data and timing information corresponding to a non-binary digital signal representative of the possible computation outcomes for Q and R

Table 1 Markov chains for high information capacity data transfer

Markov chain		
Name	Description	A_χ
simpleThis	Simply Ergodic	22
biGraphThis	Simply Ergodic	16
ThisWords	Simply Ergodic	16
This	B-system ergodic	22
binary	B-system ergodic	2

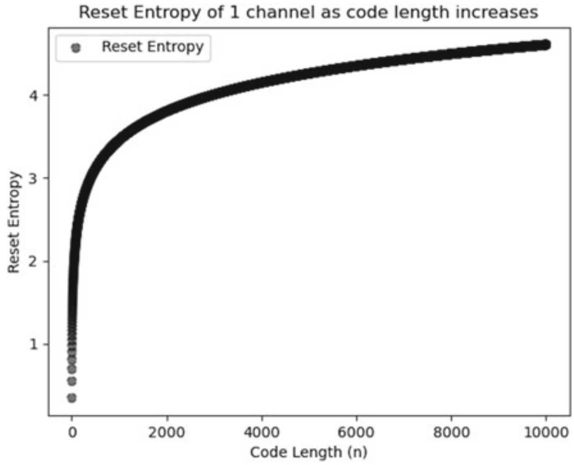


Fig. 2 The theoretical energy (reset entropy) necessary to devote to reset, when *n* possible codewords can be transmitted on 1 wire

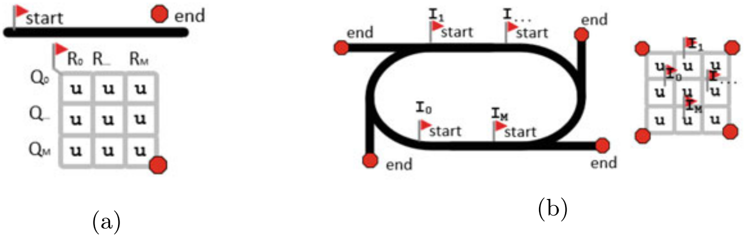


Fig. 3 **a** 1D race, has a single start and end point, with stationary computation signals in vectors R and Q. **b** 2D race, has multiple start and end points with a stationary communication system of a shared racetrack

2.2 Unit Cell and Entropy

Self-resetting domino logic circuits Self-resetting domino logic is a CMOS implementation that was developed with the motivation of 'speed up the slow signals' instead of the conventional approach of latch-based design which has the motivation to 'slow down the fast signals.' [29, 30]

An atomic event gate is a self-resetting domino logic circuit for emitting a spike event, oscillation of spike events or no event, dependent upon input A, A1. With two input event ports A and $A1$ and an output event port x and an additional port xE for the early event, this is a minimum number of inputs for a race logic `unit cell` $\mathtt{u}_2$. When unit cells built with self-resetting domino logic are interconnected into 2D race tracks, the resulting output is a sparse spike train that still maintains entropy close to the original image frame or streaming series of image frames. A self-resetting domino logic looping race track circuit is used as the basis for our experiments with 2D race tracks shown in Table 1.

3 Main Results

Race logic permits the encoding of large ($A_\chi > 2$) alphabet's upon multiple wires, and additionally, it permits the encoding of additional symbols as phase relations between the different wires. [15, 20]

When the communication between unit cells is handled through analog-to-(non-binary-digital) (hardware-to-software or hardware-to-hardware) or (binary-digital)-to-(non-binary-digital) (software-to-hardware or software-to-software), an energy-to-entropy cell equivalence is defined as the energy and time to reset the unit cell. The circuit designer can assume 1 pulse contains 1 'unit' of information. The layer of abstraction where energy use is a justifiable stand-in for information capacity makes a stable starting point for building low-energy analog-to-(non-binary-digital) signals in hardware.

The values for A_χ shown in Table 1 allow for generously long code words when compared to reset entropy predicted in Fig. 2. By modifying the encoding of symbols from our dataset to fit into a binary encoding scheme with equal weight and then to further extend that into a non-binary encoding scheme based on rate and phase, we are able to generate a spike train with a higher estimate of entropy and a higher known figure of entropy when compared to binary encoding.

Having high entropy spike trains is valuable because it indicates there could be a large amount of information present.

A non-binary communication channel can seem to accept 'compressed' data and decode into a binary memory. The compressed data is just an address-event representation of the original data, from a known information source encoder and decoder pair.

To demonstrate how this works, we created an example, depicted in Fig. 4 which starts with a streaming video and produces a list of events taken from a 2D encoding race track.

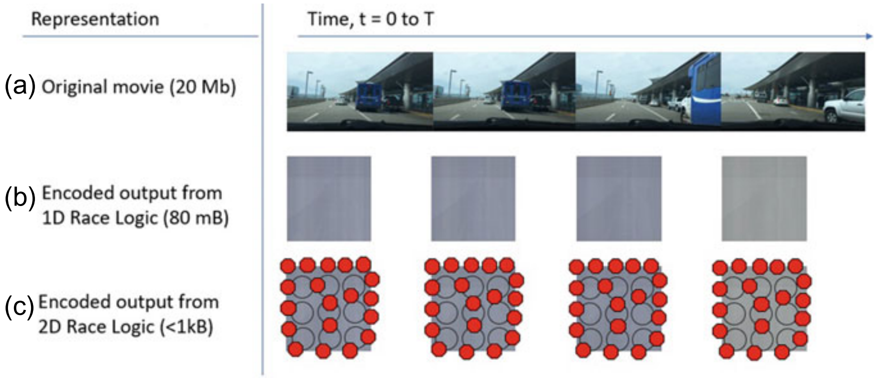

Representation
Time, t = 0 to T
(a) Original movie (20 Mb)
(b) Encoded output from 1D Race Logic (80 mB)
(c) Encoded output from 2D Race Logic (<1kB)

Fig. 4 The representation shown, to the left of the time series, lists the data formats the movie is maintained in and the average size of that data in bits. **a** Original Movie 20 Mb. **b** Encoded output from 1D Race Logic 80 mB. **c** Encoded output from 2D race logic <1 kB

Comparing an AER representation of an image frame or a series of image frames vs a png or a series of PNG (i.e., movie type), the AER representation is order of magnitudes less.

3.1 Methods

To establish a phase code for the two binary symbols 0 and 1. This can be accomplished by receiving a driving signal on one wire and emitting an outgoing signaling with three wires (channels) at minimum, which then signal a 0 by spiking in a cyclic order from $w_0 \longrightarrow w_1$, $w_1 \longrightarrow w_2$, $w_2 \longrightarrow w_0$ as long as the 'driving' symbol is 0. When the driving symbol is 1, the spikes emerge in the opposite order from the three wires $w_0 \longrightarrow w_2$, $w_2 \longrightarrow w_1$, $w_1 \longrightarrow w_0$. The relation between the single incoming signal wire and the outgoing 3 wires is that the 3 output wires encode the original signal into a non-binary digital code, which in this case, transmits $1/3$ bit per event.

To estimate the spike train entropy for a non-binary digital encoding, the authors use natural language to form the basis of a hierarchy of codes following the form of 'phrase,' 'word,' 'letter,' 'binary.' Two phrases with equivalent meaning, but different letters are selected to start. Then, the letters for each phrase are converted to binary representation using a balanced code with equal numbers of 1 and 0 with different orderings to represent a letter. Each letter represents a unit cell in a 2D Race Logic unit cell shown in Fig. 3b. The representation is only there through assignment of an identity by the circuit designer. The figures shown below with either 2 or 32 channels demonstrate how the estimate 'fails' and defaults to a maximum estimate when the code length is less than the number of channels. (Fig. 5b) The over estimate is only found when the driving symbol labeled **info** is a single character 0 or 1 to indicate the direction traversed by phase code.

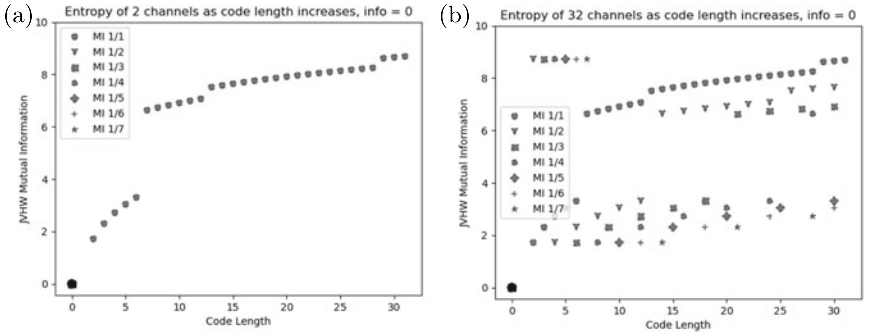


Fig. 5 **a** JVHW Mutual Information estimate of a phase code generated from a stationary Markov Chain with binary (2) channels. The estimate 'fails' and defaults to a minimum estimate when the code length is less than the number of channels used to encode the data. The 'fail' is not noticeable with binary encoding. **b** JVHW Mutual Information estimate of a phase code generated from a stationary Markov Chain with 32 channels. The over estimate is present with a mutual information around 9 for short code lengths

4 Proofs and Generated Data

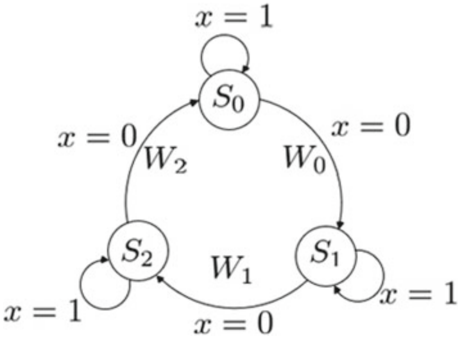
4.1 Theorem 1

A low-energy spike train response can directly correspond to the entropy of the incoming spike train. The work assumes a spike is represented by a physical pulse. **Proof** Finite state machines (FSM) are design elements used in Boolean logic to describe the behavior of a timed digital system. The states $\{S_0, S_1, S_2, ...S_n\}$ are assigned binary labels, and the transitions occur dependent upon the inputs $x_0, x_1, x_2, ...x_{N\text{inputs}}$ and the present state S_{present}.

A Markov chain is also a design element with unique stationary states $\{S_0, S_1, S_2, ...S_n\}$. It is a dynamical system $(\Omega, \mathcal{B}, P, T)$ that is *stationary* if $P(T^{-1}G) = P(G)$. The changing of states is governed by a fixed probability $P(S, \cdot)$ of transition between stationary states taken from a finite set Ω. A finite Markov chain has the property that the transition matrix P with dimensions of $\Omega \times \Omega$ is sufficient to describe it because the sequence of prior transitions leading up to the present state does not change the future states.

$$P = \begin{bmatrix} p_{S_0S_0} & p_{S_0S_1} & p_{S_0S_2} \\ p_{S_1S_0} & p_{S_1S_1} & p_{S_1S_2} \\ p_{S_2S_0} & p_{S_2S_1} & p_{S_2S_2} \end{bmatrix} \tag{5}$$

Fig. 6 A FSM transits through stationary states dependent upon the input x



Practical implementations of Markov chains are, by necessity of finite time, forced to place limits on the time that the 'fixed' probability is able to remain so. The limit comes from the noise sensitivity of the measurement system. The finite state machine illustrated in Fig. 6 has noise corresponding to the measurement of x.

Asymptotically mean stationary (AMS) provides $\bar{P}$, a stationary mean of P, which is a probability measure under which the *noise is not a problem* and the Markov chain is stationary.

$$\bar{P}(G) = \lim_{n \longrightarrow \infty} \frac{1}{n} \sum_{n-1}^{k=0} P(T^{-k}G) \tag{6}$$

The smallest probability measure that could be achieved is dependent upon an AMS source $\{\chi_n\}$. $\sigma(\chi_n, \chi_{n+1}, \chi_{n+2}, ...)$ denotes the σ-field generated by the random variable χ_n, ..., that is, the smallest σ-field with respect to which all these random variables are measurable. The finite state machine in Fig. 6 only transitions at a change in x, meaning for that FSM to be stationary, the digital circuit needs to check x at a known periodic sampling rate.

A palimpsest code conveys several types of information simultaneously, and the content of the information is able to continuously evolve to best respond to the incoming stimuli. [4] The state machines designed in this work are producing palimpsest codes.

5 Conclusion

The notable contribution of the theorem indicating a information is physical relation to reset entropy developed in Fig. 2 allow for advances in data reduction for streaming video.

Low-energy non-binary digital circuit implementations of sparse spike train encodings are capable to represent high information and high entropy signals with a much reduced datastream when compared to existing digital data formats. The supporting entropy measurements from Fig. 5b combined with the racetrack interconnect topologies presented in Fig. 3b are novel hardware software interfaces for neuromorphic engineering.

References

1. Berge HKO, Hafliger P (2007) High-speed serial AER on FPGA. In: 2007 IEEE international symposium on circuits and systems pp 857–860. https://doi.org/10.1109/ISCAS.2007.378041, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4252770
2. Berkovitz J, Frigg R, Kronz F (2006) Stud History Philos Sci Part B Stud History Philos Mod Phys. The ergodic hierarchy, randomness and Hamiltonian chaos 37(4):661–691. https://doi.org/10.1016/j.shpsb.2006.02.003
3. Davey N, Calcraft L, Adams R (2006) Connection Sci. High capacity, small world associative memory models 18(3):247–264. https://doi.org/10.1080/09540090600639339
4. Eurich C (2003) Neural dynamics and neural coding (November) 1–195
5. Falahatgar M, Orlitsky A, Pichapati V, Suresh AT (2016) Learning Markov distributions: does estimation trump compression? In: IEEE international symposium on information theory—proceedings, 2016-August, pp 2689–2693 (2016). https://doi.org/10.1109/ISIT.2016.7541787
6. Gallego G, Delbruck T, Orchard G, Bartolozzi C, Taba B, Censi A, Leutenegger S, Davison A, Conradt J, Daniilidis K, Scaramuzza D (2019) Event-based vision: a survey pp 1–26. https://doi.org/10.1109/TPAMI.2020.3008413, http://dx.doi.org/10.1109/TPAMI.2020.3008413
7. Hartley RVL (1927) Information and transmission
8. Iyer LR, Chua Y, Li H (2018) Is neuromorphic MNIST neuromorphic? analyzing the discriminative power of neuromorphic datasets in the time domain pp 1–23. http://arxiv.org/abs/1807.01013
9. Jiao J, Venkat K, Han Y, Weissman T (2015) IEEE Trans Inf Theory. Minimax estimation of functionals of discrete distributions 61(5):2835–2885. https://doi.org/10.1109/TIT.2015.2412945
10. Kendall J, Pantone R, Manickavasagam K, Bengio Y, Scellier B (2020) Training end-to-end analog neural networks with equilibrium propagation. pp 1–31
11. Liu H, Moeys DP, Das G, Neil D, Liu SC, Delbrück T, Dataset A (2016) Combined frame- and event-based detection and tracking. IEEE international symposium on circuits and systems pp 2511–2514. https://doi.org/10.1109/ISCAS.2016.7539103
12. MacKay DJC (2005) Information theory, inference, and learning algorithms
13. Madhavan A, Sherwood T, Strukov D (2014) Race logic: a hardware acceleration for dynamic programming algorithms. In: Proceedings—International symposium on computer architecture, pp 517–528. https://doi.org/10.1109/ISCA.2014.6853226
14. Madhavan A, Sherwood T, Strukov D (2015) Race logic: abusing hardware race conditions to perform useful computation. IEEE Micro 35(3):48–57. https://doi.org/10.1109/MM.2015.43, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7106377
15. Madhavan A, Sherwood, T, Strukov D (2017) A 4-mm 180-nm-CMOS 15-Giga- cell-updates-per-second DNA sequence alignment engine based on asynchronous race conditions. In: CICC
16. Miller M, Brewer F (2013) Formal verification of analog circuit parameters across variation utilizing SAT. Design, automation & test in Europe conference & exhibition (DATE), 2013 pp 1442–1447. https://doi.org/10.7873/DATE.2013.294, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6513740
17. Miró-Amarante L, Gómez-Rodríguez F, Jiménez-Fernández A, Jiménez-Moreno G (2017) A spiking neural network for real-time Spanish vowel phonemes recognition. Neurocomputing 226(March 2016):249–261. https://doi.org/10.1016/j.neucom.2016.12.005, http://dx.doi.org/10.1016/j.neucom.2016.12.005

18. Mishra U (2007) Semiconductor device physics and design. Springer
19. Nyquist H (1924) Certain factors affecting telegraph apeed
20. Payvand M (2016) Area-efficient neuromorphic silicon circuits and architectures using spatial and spatio-temporal approaches. Ph.D. thesis
21. Richardson TJ, Urbanke RL (2001) IEEE Trans Inf Theory. The capacity of low-density parity-check codes under message-passing decoding 47(2):599–618. https://doi.org/10.1109/18.910577
22. Kulkarni SR (2002) Information, entropy, and coding. In: Lecture notes for introduction to electrical signals and systems
23. Scellier B, Bengio Y (2017) Front Comput Neurosci. Equilibrium propagation: bridging the gap between energy-based models and backpropagation 11:1–21. https://doi.org/10.3389/fncom.2017.00024
24. Shannon CE (1948) A mathematical theory of communication. Bell Syst Tech J 27(July 1928):379–423. https://doi.org/10.1145/584091.584093 http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf
25. Shokrollahi A (2006) IEEE Trans Inf Theory. Raptor codes 52(6):2551–2567
26. Smith JE (2017) Space-time computing with temporal neural networks. Synth Lectures Comput Archit 12(2):i–215. https://doi.org/10.2200/S00771ED1V01Y201704CAC039, http://www.morganclaypool.com/doi/10.2200/S00771ED1V01Y201704CAC039
27. Tzimpragos G, Madhavan A, Vasudevan D, Strukov D, Sherwood T (2019) Boosted race trees for low energy classification. In: International conference on architectural support for programming languages and operating systems—ASPLOS, pp 215–228. https://doi.org/10.1145/3297858.3304036
28. Tzimpragos G, Michelogiannakis G, Volk J, Shalf J, Sherwood T (2020) A computational temporal logic for superconducting accelerators, pp 435–448
29. Winters BD, Greenstreet MR (2002) A negative-overhead, self-timed pipeline. In: Proceedings—International symposium on asynchronous circuits and systems
30. Winters BD, Greenstreet MR (2003) Microprocess Microsyst. Surfing: a robust form of wave pipelining using self-timed circuit techniques 27(9):409–419. https://doi.org/10.1016/S0141-9331(03)00091-7
31. Wu Y, Zhao R, Zhu J, Chen F, Xu M, Li G, Song S, Deng L (2020) Brain-inspired global-local hybrid learning towards human-like intelligence, pp 1–34. ArXiv.org
32. Yu T, Park J, Joshi S, Maier C, Cauwenberghs G (2012) 65K-neuron integrate-and-fire array transceiver with address-event reconfigurable synaptic routing. In: 2012 IEEE biomedical circuits and systems conference: intelligent biomedical electronics and systems for better life and better environment, BioCAS 2012—conference publications, pp 21–24. https://doi.org/10.1109/BioCAS.2012.6418479

Investigations into Secure IaC Practices

Keerthi Neharika and Ruth G. Lennon

Abstract Security is one of the major concerns for companies, as security attacks are rapidly increasing. There are many laws and regulations which provide guidelines to companies for securing their applications. A few of those laws impose heavy fines when appropriate measures for security are not taken. Provisioning infrastructure using manual configuration can also be a difficult task as it involves multiple steps. In this paper, we investigate securely provisioning infrastructure automatically. Security and automatic infrastructure provisioning can be achieved using source code analysis tool, container security tool, and IaC tools. We show that source code and containers can be scanned for vulnerabilities, and when critical vulnerabilities are not found, the infrastructure can be automatically provisioned using Terraform script. The authors observed that implemented systems can be scanned for vulnerabilities in source code and containers provisioned automatically using secure IaC script.

Keywords Infrastructure as code · DevOps · Automation

1 Introduction

For some time, the information technology (IT) infrastructure was provisioned manually, which means people had to get physical servers and do the configuration process manually. This technique incurred high costs and was inflexible. As the size of infrastructure grew, an effective technique, which would reduce the complexity of infrastructure provisioning and management, was required. Infrastructure as code (IaC) is the management of infrastructure components like load balancers, virtual machines (VMs), and networks through code. It involves automation rather than the manual process which can reduce errors. Scripted solutions did exist prior to DevOps, but they were not always easy to understand with; only, the author was able to read

K. Neharika (✉) · R. G. Lennon
Letterkenny Institute of Technology, Letterkenny, Ireland
e-mail: l00161834@student.lyit.ie

R. G. Lennon
e-mail: Ruth.Lennon@lyit.ie

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_25

them [1] in many cases. Automating such tasks is considered key to implementing DevOps. Companies such as GitHub, Google, Netflix, and Facebook adopted IaC due to its effectiveness [2].

The core idea behind the approach of IaC is writing and using code to define, deploy, and update the infrastructure to enhance repeatability at speed [3]. The technology of IaC and the related practices emerged along with the introduction of cloud computing, more specifically with infrastructure as a service (IaaS). IaC is often considered to support software development practices such as agile software development and more closely support practices related to DevOps. However, we argue that many of the guiding principles of the SDLC as set out in the DevOps standard should be applied to the IaC itself.

Coming from Agile culture, DevOps sets as one of its priorities frequent feedback loops which are augmented by continuous development and the deployment so that rapid delivery can be achieved. Given the variety of customer demands and the quickly changing marketplace, one of the most common requirements of software engineering is agility [4] in adapting to change. Hence, several agile methodologies including Scrum and Kanban have become prevalent for development. However, this can bring additional security risks to the process of software development.

Although DevOps results in faster software delivery, a concern is that software might not undergo sufficient security-related reviews. Software security was one of the major concerns of companies, specifically when cyber-crimes have increased. Hence, many enterprises and practitioners intend to integrate security into DevOps by adopting best practices related to security and by training the developers [5]. These events triggered a new term, DevSecOps. Companies can achieve high-quality software by introducing security principles in the process of DevOps throughout the lifecycle of software. Security is a first-class citizen of the SDLC in DevOps, but with DevSecOps, higher visibility is afforded to the topic.

Many disciplines regarding overall quality improvement including test-driven development, automation of built and deployment, and continuous integration are gaining traction. The major focus however with infrastructure is its ability to support the software rather than the IaC itself [6]. Once the initial infrastructure configuration is set up, multiple changes may be required even before going into the production environment. In few cases, infrastructure might not be well planned to meet requirements. It can be difficult to build the whole infrastructure again when carried out manually; hence, IaC was introduced. The process of applying a clear strategy for the SDLC of the IaC is not always considered. Further, adding security to the process is not often a key consideration.

Two of the biggest challenges which DevOps bring to security are education on security and environmental risk. Due to vulnerabilities in code, serious problems might occur; flaws contained in the code can create potential risks and compromise security. These flaws can enable hackers and attackers to take advantage of the code; they might attach an endpoint to extract the valuable data, the software be tampered, and the whole data can be erased. Vulnerable code can make both user and developer vulnerable; once an attack occurs, everything can be lost. The vulnerability which arises from the underlying source code must be detected and removed in such a way that the applications are safe from all types of attacks. Research was conducted by CAST Research Labs, where they found that the average number of security flaws in .NET, and Java applications are approximately between 30 and 100 per 10K lines of code [7]. As yet, there is insufficient research into the number of security flaws in IaC programming languages.

Detecting the potentially vulnerable code is one of the important steps in the software development life cycle. This process might help the security experts to remove the vulnerabilities in the code thus protecting the infrastructure. Vulnerabilities can be one of the major threats to security; however, detecting the vulnerabilities in code is a challenging task [8]. This is more so in IaC with suppression statements as one example of how a security risk can be easily missed. It is difficult to adjust to consider comments having such control over the underlying systems. It can be more difficult to change our culture to consider the risks in comments as well as core coding structures.

Additionally, containers can also have some vulnerabilities which must be detected and removed. More work has been covered on the various aspects of container security. Again, however, security of the code to provision containers may not be tested as well as the containers themselves. Overall, there is a strong need for a solution that can detect the vulnerabilities in code during all stages of software development and can detect vulnerabilities in IaC.

It might not always be practical, efficient, or user-friendly to use some commercial management consoles. Creating a VM using one of the public clouds like Amazon Web Services (AWSs) or Microsoft Azure involves going through more than four forms, and users might have to fill more than 25 fields. Additionally, the VMs might be created and removed many times a day during the development and test phases; doing all these tasks manually might not be viable.

In traditional approaches, application software was installed on the system nodes. Each node was patched individually; the software is updated; network configuration and other parameters will be changed as per the requirement [9]. In few cases, nodes might be created only using a backup, and there will not be an ability to reconstruct the configuration from the start. Whereas, IaC enables the practice of IT operations named immutable infrastructure. In this infrastructure, changes in configuration, patches, and updates will not be applied to the deployed nodes. Instead of this process, a whole new version of the IaC code will be created with all the required modifications which reflect the required changes to the deployed applications.

2 Background

2.1 DevOps

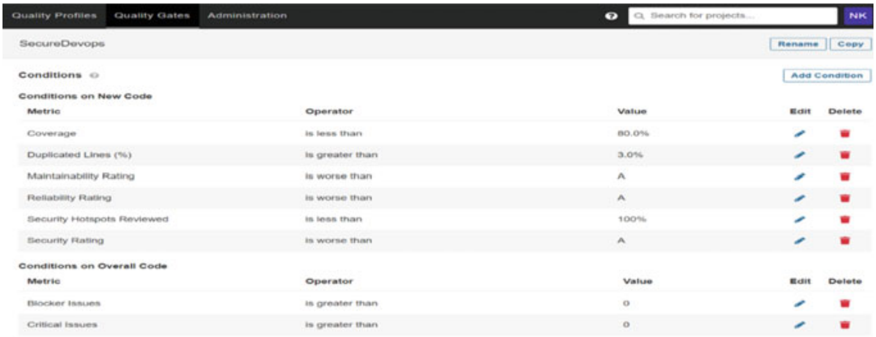
DevOps is a collaborative effort in an organization providing reliability through automating continuous delivery of software. DevOps encourages collaboration between not only operators and developers but all relevant stakeholders. This point is often missed when discussing the concept. For this reason, security is not always considered a core concept of DevOps. Some agile processes became inefficient due to conflicts between developers and operators often borne form poor understanding of terminology or lack of communications. Additionally, there can be pressure of scheduled deployment times, and the requirement of frequent releases. It is estimated that DevOps processes drive more than 80% of the industry-strength technology in the market [10].

The term DevOps was first invented in the year 2009 by Patrick Debois while organizing a conference called DevOpsDays, a series of conferences, which ultimately helped spread of the term's popularity [11]. Separation of the operations of software from its development through siloed thinking leads to many issues, due to lack of integration, communication, and collaboration. These issues could lead to delays in the build process which could take hours for a given application. The situation is vastly different with DevOps where developers can start the builds irrespective of the time, and the results can be achieved rapidly. Unfortunately, not everyone took the time to consider how DevOps reference to left shift must include security as well as quality aspects.

It is possible for developers to commit code into the production without communicating to other development teams in the organization, the design choices and architectural style or justification for these decisions. On their way to production, systems may pass through several environments, affecting the use of configuration parameters [12]. Without enhanced communication this information, often critical to security, can be lost. The approach of DevOps is often paired with the agile methodology and lean principles of software development. This aids multiple domains such as development, operations, security, quality assurance, and business owners to collaborate such that the delivery of software can be done uninterruptedly. DevOps enhances the way that a business delivers value to its suppliers, partners, and customers [13].

2.2 DevSecOps

In traditional methods of delivery, code from the development team is security checked prior to being merged into the final build. At this point, bugs could be detected, which are difficult to fix. These bugs might be left unfixed due to pressures regarding the product release dates and deadlines; lack of security will be detected after the stage of quality assurance test; security methods might be left unimplemented in such cases. In a software development lifecycle with security at the end, the applications will be built in an insecure way in most cases [14]. DevSecOps, which expands to development, security, and operations, change the structure of the application lifecycle such that security has increased visibility in the SDLC. The aim is to ensure security is considered at every step. When security checks are enforced, such as with gating shown in SonarQube in Fig. 1, potential vulnerabilities can be detected, and appropriate actions are taken [15].



SecureDevops

Conditions

Conditions on New Code

Metric	Operator	Value	Edit	Delete
Coverage	is less than	80.0%	✎	🗑
Duplicated Lines (%)	is greater than	3.0%	✎	🗑
Maintainability Rating	is worse than	A	✎	🗑
Reliability Rating	is worse than	A	✎	🗑
Security Hotspots Reviewed	is less than	100%	✎	🗑
Security Rating	is worse than	A	✎	🗑

Conditions on Overall Code

Metric	Operator	Value	Edit	Delete
Blocker Issues	is greater than	0	✎	🗑
Critical Issues	is greater than	0	✎	🗑

Fig. 1 Security gates as well as quality gates for IaC

There is existing support for the application of security. The International Organization for Standardization (ISO) 27001 is an information security management system (ISMS), provides an overview of security assurance programs at the organization level. It does not provide a technical approach but offers security management programs. ISO 27001 specifies security practices of DevOps, including cryptography, operation security, compliance, access control, and software development. This provides a guideline to develop individual DevOps security programs [16].

One alternative to reduce risk is to reduce the speed of change to enable greater time to support quality and security reviews. Although reducing the risk is a valid aim, this technique could not address the requirements of businesses that are fast-moving and technology dependent. The concept of DevSecOps was coined by Neil McDonald of Gartner where he acknowledged that security was required, but stated that effort of DevOps must not be reduced in the favor of security [17]. He addressed this problem by stating that the security should be integrated into DevOps.

This idea was effective but contradictory to security practices of many of the security organizations. The security teams are required to collaborate with development and operations and introduce some conditions of test, and quality on production code pushes without impacting the process time. When security metrics and parameters integrated into test and development qualifications, then, the possibility of security getting involved becomes higher. Security teams can collaborate with development and quality assurance teams to discuss the key qualifiers and parameters which need to be met before the promotion of code. Additionally, they must integrate the automated static and dynamic testing of code throughout the life cycle of development and promotion. With the automated tests, security and development teams can detect and fix big flaws in the code [17].

DevSecOps can be characterized by the four pillars of DevOps; the first pillar is culture; in security, this means the creation of a company culture where security is considered as the responsibility of everyone. It can also mean, involving the security team in the development process. In relation to tools, this means using shared interfaces where security staff and developers use to maintain the track of vulnerabilities. Automation is using tools for automating security testing, such security checks are known as ‘Security as a Code’. Automatic security processes enable the processes to be scalable and predictable. When automatic tests are configured, developers can spend more time writing the code instead of handling the tests.

There are few challenges of DevSecOps; companies show negligence toward security, and the developers become unhappy due to the reduction of autonomy. Lack of appropriate tools, standards, and technologies regarding the usage of tools and lack of security education of developers can be a challenge for DevSecOps.

2.3 Security Standards and Regulations

There are many standards and regulations that are applicable in this space. Not all are either implemented or recognized as to their applicability. Certainly, it is important to view the work of the OWASP foundation and the top 10 which continues to be proven applicable year on year. Further, standards for quality can be found in the IEEE 2675 DevOps standard for building Reliable and Secure Systems including Application, Build, Package, and Deployment. The focus of this standard is to establish better IT controls and compliance. The standard also specifies DevOps principles and detail ways for effective collaboration of developers, stakeholders, and operations staff [18]. In DevOps, taking a broad view enables professionals of technology to understand the system completely [19].

The regulations of General Data Protection Regulation) (GDPR) highlight the protection of sensitive data of the customers stored and processed by the organizations. The data of customers can only be secure when the systems in which it is stored and processed are designed efficiently. When security is not integrated into DevOps, companies may be vulnerable to attacks and security breaches. It is a common perception that integrating security in the development process reduces the speed of software development, but this might not be the case in all situations. It increases the code quality, helps companies to maintain security, and prevents expensive rewrites of applications.

2.4 Infrastructure as Code (IaC)

IaC’s impact becomes more apparent when you consider the steps that are repeated many times across multiple servers. IaC uses high-level languages to code versatile provisioning of resources. Infrastructure as code has its own software development lifecycle just as with other software. Various stages of software development, therefore, become repeatable, error-free [20] for IaC as well as other parts of the SDLC. Infrastructure designs, scripts, models, dependencies, configuration code, and parameters can be expressed using one language [6] with appropriate process and procedures to ensure quality.

Defective IaC scripts can have serious complications and consequences. For example, in 2017 January, execution of a defective IaC script erased home directories of approximately 270 users in the cloud instances which are maintained by Wikimedia. As another example, in 2017, Amazon Web Services (AWSs) faced an outage worth 150 million USD due to a defective IaC script. IaC offered many benefits for IT companies; a company surveyed users in the year 2016 and reported that IaC scripts helped organizations gain 210% in time savings. National Aeronautics and Space Administration (NASA) saved around 45 min in the patching process by using IaC scripts [21].

2.5 IaC Security

While writing IaC scripts, developers might accidentally introduce security smells. A security smell can be a coding pattern that indicate security weaknesses and can lead to breaches. IaC scripts which consist of hard-coded credentials or other security smells can be vulnerable to security attacks or breaches. A few of the security smells which might occur in IaC scripts are explained below.

1. Administrative access by default: In this security smell, default users can be given administrative access. This smell breaks the principle of least privilege, which suggests designing and implementing the system which provides only the least access for users.
2. Comments: The pattern of including information regarding system weaknesses, defects, and other information in the comments can be problematic [22].
3. Cryptographic algorithms: This security smell can be occurred when weak cryptographic algorithms are used. Few algorithms can suffer from security-related issues and can be vulnerable to security attacks.
4. Hard coding the secrets: This can disclose sensitive information like passwords and usernames in the form of configuration within IaC scripts. Within IaC scripts, the configuration of the system can be specified. When programmers hard code such confidential information in scripts, it can lead to security issues.
5. IP Addressing: This smell can occur when inappropriate IP addresses are assigned for servers. For instance, using IP address with all zeros might cause security problems as this IP address accepts connections from every network by default [23].

Static Code Analysis The method of examining the structure of a program or software product which is at an intermediate level is known as static analysis. This process is usually automated which can find out errors and defects in the software products. Static code analysis concentrates on scanning the source code of the software. The major focus of this type of code analysis is to scan the elements of the programs, the structure of the program, and the program behavior. The process of analyzing the data flow of the program involves examining where the data arrives from and where it goes; it also analyzes how the code deals with the data. The control flow examines the paths which can be taken by a program; these paths are generally represented by a control graph. Static analysis platforms examine the source code without running the program.

Dynamic Code Analysis To check the behavior of the program, this type of code analysis executes the program. The method of debugging by analyzing the application while the program is running is known as dynamic code analysis. This type of analysis can give information that can help in troubleshooting production incidents rapidly. This can also be used in a preproduction environment as it prevents unsafe or vulnerable code from going into a production environment [24].

3 System Under Test

To demonstrate the problems stated in the previous sections including the application of DevOps practices applied to the IaC SDLC, a system is presented here. The system was tested using different test cases by introducing vulnerabilities into the source code. The main aim of this research was to identify whether infrastructure be securely provisioned in an automatic way using IaC tools. This research is still in early phases. Initial tests are described here, but further research is currently under way.

The system consists of a version control system where DevOps teams can commit code. The source code which gets committed to version control system goes through vulnerability scanning. Additionally, when containers or container images are used in the system, these will also be scanned for vulnerabilities. The infrastructure can be provisioned when the security checks are complete, and there is no potential risk.

The system, see Fig. 2, consists of GitHub where development teams can commit code and Jenkins for creating the pipeline. The system also contains SonarQube and Trivy for securing the system by performing vulnerability scanning. To provision the infrastructure automatically, Terraform was used.

Ubuntu OS was used for the implementation, Docker engine for Ubuntu and Jenkins was installed in it. Terraform and curl packages were installed; these packages are necessary to verify the GPG signature of HashiCorp. Debian package repository was installed, and the HashiCorp GPG key was added. HashiCorp Linux repository was added, and Terraform CLI was installed and verified.

To integrate GitHub projects with Jenkins, a Webhook was added using GitHub repository settings. Uniform resource locator (URL) of the Jenkins environment was added, and other fields were filled using suitable options. The events which are to be triggered by the Webhook were selected manually based on the requirements. A new project was created in Jenkins by giving it an appropriate name, and the URL of the GitHub repository was given. Required build triggers were added; integration of the Jenkins project with the GitHub repository was done. To integrate Jenkins with Docker, Docker Hub credentials were added. To add the credentials, the ‘Add new credentials’ option was selected; username and password were entered.

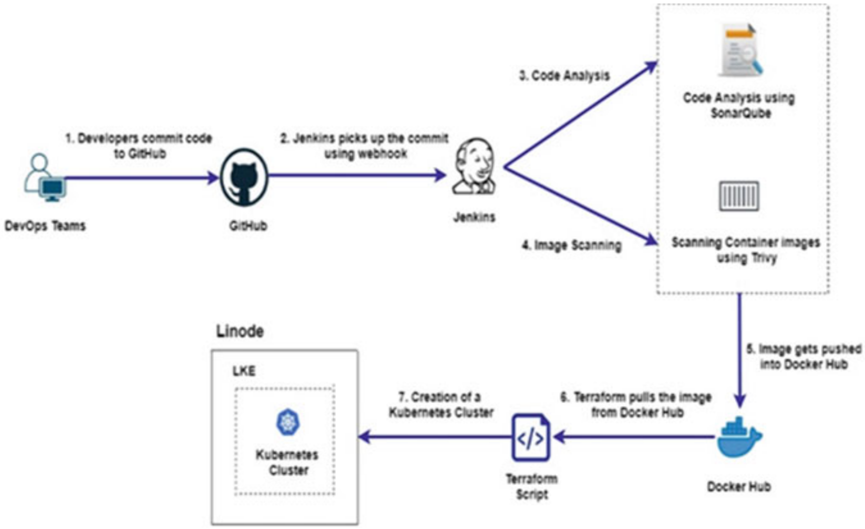

1. Developers commit code to GitHub
2. Jenkins picks up the commit using webhook
3. Code Analysis
4. Image Scanning
Code Analysis using SonarQube
Scanning Container images using Trivy
DevOps Teams
GitHub
Jenkins
5. Image gets pushed into Docker Hub
Linode
LKE
Kubernetes Cluster
7. Creation of a Kubernetes Cluster
6. Terraform pulls the image from Docker Hub
Terraform Script
Docker Hub

Fig. 2 System architecture

SonarQube analysis when it must be done regularly, or after every task, it can be difficult to perform the analysis manually. To address this problem of manual analysis, SonarQube can be integrated with Jenkins. When both platforms are integrated, automatic SonarQube analysis can be configured. Sonarqube was integrated with Jenkins. Server authentication token of SonarQube was required in Jenkins for integration which provides additional security to the pipeline. After completing the integration, a job was created to create a report of the project. This is important to provide a log of activities carried out.

To create a Kubernetes cluster, Linode Kubernetes Engine (LKE) was used. It provides a Kubernetes service and completely manages the cluster control plane. Terraform script was used to create the Kubernetes cluster. In the script, details of the required resource to be created within Linode were specified using a script. Variables for k8s_version, label, region, and tags were created, and default values were declared. As the Docker image was pushed to the private repository, Terraform must be configured such that it can get account details while pulling the image. Docker was logged in, and few commands were given in the Terraform folder. Care must be taken to ensure that 'secrets' are used to add a layer of safety to the configuration properties.

As per the system design and implementation, when code gets committed into GitHub, Jenkins must pick up the commit through Webhook. The source code must be scanned for vulnerabilities by SonarQube, and then, containers must be scanned by Trivy. When there are no critical vulnerabilities or blockers, the image must be pushed into Docker hub. Terraform must then pull the image and create a Kubernetes cluster in Linode.

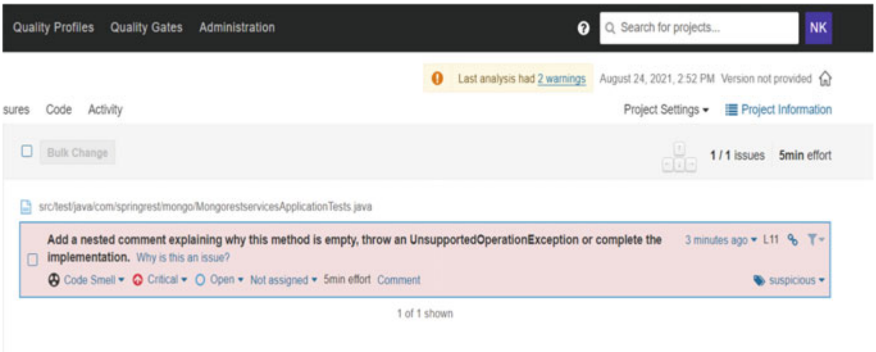
The system was tested in various exemplar aspects, according to the implementation. When code is committed to GitHub repository, SonarQube must scan the code and provide details about detected vulnerabilities blockers, critical, minor, and major issues. Initially, sample code was committed to test the SonarQube implementation. The tool scanned the source code and listed all the vulnerabilities according to their severity. The tool detected that the committed code does not contain any blockers or critical issues. In addition to detecting the vulnerabilities, SonarQube also offered suggestions to solve the issues detected (Fig. 3).

The tool also provided the overall status of the committed code, which displayed the result of the quality gate. The quality gate step in the Jenkins build passed because the quality gate was configured in such a way that whenever there are greater than zero blockers or critical vulnerabilities, the quality gate must be failed. Jenkins pipeline was created in such a way that whenever the quality gate fails, the next step within the pipeline fails, and as a result, the complete pipeline fails.

To test SonarQube implementation, further, a vulnerability was introduced into the code which was used in the previous test. The changed code was committed; a new build was triggered in Jenkins. SonarQube scanned the code and detected one critical vulnerability that might create a severe security problem. A critical vulnerability was detected by it. As the vulnerability was critical, the next step in the pipeline could not pass, and hence, the built was failed.

The overall security and reliability of the code can be reviewed through the tool. It plotted the results on a graph. As seen in the image, it also assigned ratings for the new code and the overall code. These ratings enable users to understand the security level and quality of the code at one glance (Fig. 4).

After testing the implementation of SonarQube, Trivy was applied to further test security. Once code analysis is completed, and there are no critical vulnerabilities or blockers, Docker images must be scanned. A container image was added into the code, and the code was committed into Github. In the initial tests, Trivy successfully scanned the container image but showed no vulnerabilities in the image. In the next stage of testing, a Docker image containing vulnerabilities was added, and



Last analysis had 2 warnings August 24, 2021, 2:52 PM Version not provided

1 / 1 issues 5min effort

src/test/java/com/springrest/mongo/MongorestservicesApplicationTests.java

Add a nested comment explaining why this method is empty, throw an UnsupportedOperationException or complete the implementation.

3 minutes ago L11

5min effort

1 of 1 shown

Fig. 3 Detected vulnerabilities

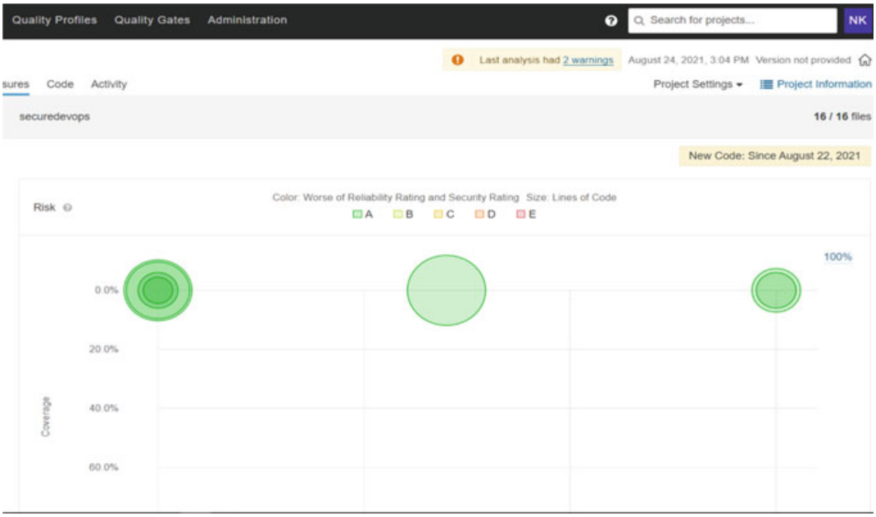


Fig. 4 High-level security rating

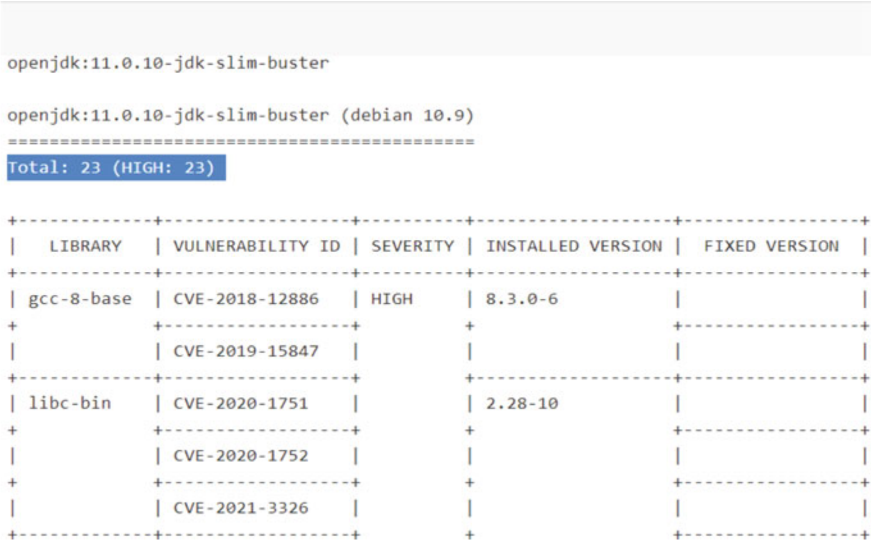
the code was committed. The container analysis tool scanned the vulnerabilities of the container image; 23 high vulnerabilities were detected in the image.

After testing code analysis and image scanning techniques, infrastructure provisioning was tested. The script was run; Terraform pulled the image from Docker repository and created an LKE cluster in Linode. Overview of the LKE cluster was checked through Linode interface.

The Jenkins pipeline was created such that when a developer commits code to GitHub, SonarQube scans the source code to check vulnerabilities. When the code does not contain any critical vulnerabilities or blockers and as the quality gate passes, Trivy scans containers (Fig. 5). When containers also do not contain major vulnerabilities, then, they gets pushed to Docker Hub. The infrastructure will then be provisioned by running Terraform script. However, when there are any vulnerabilities in source code or containers, the build fails. Using different test cases, the pipeline was tested.

4 Discussion

The integration of DevSecOps principles and practices with automatic infrastructure provisioning has been discussed at length. Implementing security mechanisms and ensuring that they are continuously maintained is the responsibility of all organizations. We have outlined that security attacks and data compromises are increasing, and many individuals are getting affected. Approximately, 98.2 million users became victims for ten biggest data breaches occurred in the first six months of 2021 [25].



```
openjdk:11.0.10-jdk-slim-buster

openjdk:11.0.10-jdk-slim-buster (debian 10.9)
=============================================
Total: 23 (HIGH: 23)

+-------------+------------------+----------+-------------------+-----------------+
|   LIBRARY   | VULNERABILITY ID | SEVERITY | INSTALLED VERSION |  FIXED VERSION  |
+-------------+------------------+----------+-------------------+-----------------+
| gcc-8-base  | CVE-2018-12886   | HIGH     | 8.3.0-6           |                 |
+             +------------------+          +                   +-----------------+
|             | CVE-2019-15847   |          |                   |                 |
+-------------+------------------+          +-------------------+-----------------+
| libc-bin    | CVE-2020-1751    |          | 2.28-10           |                 |
+             +------------------+          +                   +-----------------+
|             | CVE-2020-1752    |          |                   |                 |
+             +------------------+          +                   +-----------------+
|             | CVE-2021-3326    |          |                   |                 |
+-------------+------------------+          +                   +-----------------+
```

Fig. 5 Detected container vulnerabilities

With this information, it is evident that security is very crucial these days. While conducting the initial research, it was identified that business might have to face many problems without implementing security.

Popular standard like ISO 27001 provides guidelines for information security. Using these guidelines, different kinds of organizations can handle security of their valuable information. Using this standard, companies can have advantages like protecting the data, responding to security-related threats, and enhance the culture of company. Europe’s security and data privacy law is considered as one of the toughest privacy laws. With the rules of this law, users are given enhanced control over their personal information. GDPR imposes heavy fines and other punishments when companies fail to be GDPR compliant. PCI DSS is another security standard which was created to address the problems of payment frauds. All the service providers and merchants are advised to follow the rules set by this standard. This standard lists twelve requirements, which help in reducing payment card frauds and security attacks. Companies must complete an auditing process to show that they are PCI DSS compliant.

Recently, the IEEE 2675 standard for Building Reliable and Secure Systems, including Application Build, Package, and Deployment was released. This standard provides practices and procedures to implement DevOps at all stages of the software lifecycle regardless of the purpose of the software. Existing and new security standards and regulations prove that implementing security in IT systems is necessary.

DevSecOps highlights the role of security within DevOps including securing the infrastructure and the applications from the outset. Source code and containers images were chosen for demonstration purposes such that the vulnerabilities can be demonstrably detected. Source code vulnerabilities can provide entry points to attackers through which they can hack the systems. Vulnerabilities can occur during two of the most important phases of the software development life cycle such as design and coding. Vulnerabilities can arise because of coding and design errors or by using components with vulnerabilities. Developing complex code can also lead to vulnerabilities in some cases. Source code vulnerability scanning is important due to the increasing size and complexity of IaC. Source code scanning detects vulnerabilities in the source code and provides early opportunities to fix those flaws.

To enhance the security of the system, we believe that newly created containers also must be scanned for vulnerabilities. Automating container scanning for vulnerabilities enables detecting the vulnerabilities in the early stages. Many tools and platforms which perform container scanning, analyze all the contents within containers, and then compare the contents with the vulnerabilities which can compromise the security of the applications. Containers provide many advantages are container images can be used from public registries. However, they might not be secure to use without detailed evaluation of the image itself. Images that are tagged as official or trusted should still be scanned for vulnerabilities. Integrating a tool that can automatically perform scanning on containers can benefit the system.

An additional consequence to the use of secure IaC may be reduce costs as automating the infrastructure provisioning allows administrators to focus on key problems rather than manually testing the security of systems under consideration. This assists most particularly with misconfigurations often found with new tools or products.

During the research, several ways of implementing security were examined. It was identified that securing the source code and containers can help in securing the system. To implement source code and container vulnerability scanning, tools which can provide better features and perform efficient scanning were selected. From a review of the features of several IaC tools, source code and container scanning tools SonarQube, Trivy, and Terraform were selected to perform source code scanning, container scanning, and IaC were chosen, respectively.

If these source code scanning tools were not implemented, the build could pass the testing steps despite vulnerabilities included. SonarQube gives an overview of committed code; it displays the status of the quality gate and details of detected vulnerabilities. SonarQube also provides the overall rating for reliability, security, maintainability, and other aspects. It plots these ratings in a graph and provides its details like the number of lines of code, and the ratings. In this paper, source code vulnerability scanning was automated. Without the functionality of automatic code analysis, vulnerabilities might have to be scanned manually. In some cases, it might not be possible to detect the vulnerabilities manually due to code complexity. This automation can save time and reduce human effort. It can be very difficult to scan thousands of lines of code for vulnerabilities. All in all, the author identified that through the SonarQube tool, vulnerabilities of source code were detected. Using the suggestions given by this tool, vulnerabilities can be removed.

When the source code committed for testing does not contain any critical vulnerabilities or blockers, Trivy starts scanning containers for vulnerabilities. Checking for container vulnerabilities manually can become a complex task. The functioning of the container scanning tool and the results were explained in the previous chapters. While testing the practical artifact, it was observed that the container scanning tool enhanced the security of the system to some extent. Trivy detects vulnerabilities by examining all the components of containers. Like SonarQube, this tool also detects vulnerabilities and then segregates the vulnerabilities based on severity. The integration of these two security tools in the system can help in securely provisioning the infrastructure.

Terraform script for IaC was written by considering typical provisioning requirements. When there are no critical vulnerabilities in the source code and containers, Docker container gets pushed into the Docker hub. Linode platform provided an overview of all the servers created and Kubernetes cluster which were provisioned using Terraform script. The Kubernetes cluster was created with minimal resources due to cost issues.

In conclusion, as a part of this research, a system which can securely provision the infrastructure automatically using IaC tools was designed and implemented. It was observed that the security tools detected the vulnerabilities and enabled creation of secure system. It was also noticed that infrastructure provisioning can become efficient and simple when IaC is used as opposed to traditional approach. Many tools were involved in this paper; integrating those tools was a major task. Extensive configuration was done such that all the tools are functioning collaboratively.

5 Future Work

This paper presented the early practical work of testing secure provisioning of resources using IaC using DevOps practices. However, further testing is required. It is intended that the research is replicated using other tool providers to test the efficacy of the both the tools and practices.

References

1. Hüttermann M (2012) Infrastructure as Code. In: DevOps for developers. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4302-4570-4_9
2. Patni JC, Banerjee S, Tiwari D (2020) Infrastructure as a Code (IaC) to software defined infrastructure using azure resource manager (ARM). In: International conference on computational performance evaluation (ComPE), pp 575–578. https://doi.org/10.1109/ComPE49325.2020.9200030
3. Sandobalín J, Insfran E, Abrahão S (2020) On the effectiveness of tools to support infrastructure as code: model-driven versus code-centric. IEEE Access 8:17734–17761. https://doi.org/10.1109/ACCESS.2020.2966597
4. Lee JS (2018) The DevSecOps and agency theory. In: 2018 IEEE international symposium on software reliability engineering workshops (ISSREW), pp 243–244. https://doi.org/10.1109/ISSREW.2018.00013

5. Mao R et al (2020) Preliminary findings about DevSecOps from grey literature. In: 2020 IEEE 20th international conference on software quality, reliability and security (QRS), pp 450–457. https://doi.org/10.1109/QRS51102.2020.00064
6. Artac M, Borovssak T, Di Nitto E, Guerriero M, Tamburri DA (2017). DevOps: introducing Infrastructure-as-Code. In: IEEE/ACM 39th international conference on software engineering companion (ICSE-C), pp 497–498. https://doi.org/10.1109/ICSE-C.2017.162
7. Zaharia S, Rebedea T, Trausan-Matu S (2019) Source code vulnerabilities detection using loosely coupled data and control flows. In: 2019 21st International symposium on symbolic and numeric algorithms for scientific computing (SYNASC), pp 43–46. https://doi.org/10.1109/SYNASC49474.2019.00016
8. Du et al X. LEOPARD: identifying vulnerable code for vulnerability assessment through program metrics. In: IEEE/ACM 41st international conference on software engineering (ICSE), pp 60–71. https://doi.org/10.1109/ICSE.2019.00024
9. Klein J, Reynolds D (2019) Infrastructure as Code: final report. Software Engineering Institute. https://resources.sei.cmu.edu/assetfiles/WhitePaper/2019, 19(001), p 539335
10. Pang C, Hindle A, Barbosa D (2020). Understanding DevOps education with grounded theory. In: IEEE/ACM 42nd international conference on software engineering: companion proceedings (ICSE-Companion), pp 260–261
11. Hüttermann M (2012) DevOps for developers. Apress
12. Bass ZL, Champlin-Scharff G (2016) DevOps and its practices. IEEE Softw 33(3):32–34. https://doi.org/10.1109/MS.2016.81
13. Madane S, Dandem M. Importance of DevOps
14. Carter K (2017) Francois Raynaud on DevSecOps. IEEE Softw 34(5):93–96. https://doi.org/10.1109/MS.2017.3571578
15. Gomes KT (2018) The importance of DevSecOps
16. Hsu THC (2018) Hands-on security in DevOps: ensure continuous security, deployment, and delivery with DevSecOps. Packt Publishing Ltd.
17. Shackleford D (2016). A devsecops playbook. SANS Institute InfoSec Reading Room. A DevSecOps playbook
18. Hasan Y (2021) Announcing IEEE 2675 DevOps standard to build reliable and secure system. Available https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=653267. Last accessed 16 Aug 2021
19. IEEE standard for DevOps: building reliable and secure systems including application build, package, and deployment. In: 2021 in IEEE Std 2675-2021, pp 1–91. https://doi.org/10.1109/IEEESTD.2021.9415476
20. Fernandez T (2020) What is infrastructure as code? Available https://blog.stackpath.com/infrastructure-as-code-explainer/. Last accessed 14 July 2021
21. Rahman A (2018) Characteristics of defective infrastructure as code scripts in DevOps. In Proceedings of the 40th international conference on software engineering: companion proceedings. association for computing machinery, New York, NY, USA, pp 476–479. DOI:https://doi.org/10.1145/3183440.3183452
22. David F (2020) IaC security risks. Available https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/infrastructure-as-code-security-risks-and-how-to-avoid-them. Last accessed 17 Aug 2021
23. Rahman CP, Williams L (2019) The seven sins: security smells in infrastructure as code scripts. IEEE/ACM 41st international conference on software engineering (ICSE), pp 164–175. https://doi.org/10.1109/ICSE.2019.00033.
24. Karthik L (2020) Static versus dynamic code analysis. Available https://www.overops.com/blog/static-vs-dynamic-code-analysis-how-to-choose-between-them/. Last accessed 16 Aug 2021
25. Michael N (2021) The 10 biggest data breaches of 2021. Available https://www.crn.com/slide-shows/security/the-10-biggest-data-breaches-of-2021-so-far-. Last accessed 26 Aug 2021

ANETtE—Automated Network Evaluation and Test Environment

Christoph Uran, Valentin Egger, Kurt Horvath, and Helmut Wöllik

Abstract Continuous tests and measurements, as well as the evaluation of their results, are important tasks to ensure the smooth operation of modern computer networks. As this paper demonstrates, this is especially true for 5G research networks that encompass use cases with varying requirements. A fully automated approach to define, execute, and evaluate measurements in such a network is described. The resulting system consists of four distinct modules that are fully containerized and interact with each other based on well-defined interfaces. Furthermore, the automatic generation of comprehensible reports for different user groups is covered within this system. Thereby, the workload of the involved test engineers and the potential for errors are greatly reduced.

Keywords Network testing · Performance measurement · Reliability · Containerization · Cloud computing · 5G

The work presented here was partially sponsored by the Carinthian Agency for Investment Promotion and Public Shareholding (BABEG) using means of the Republic of Austria and the State of Carinthia.

C. Uran (✉) · V. Egger · K. Horvath · H. Wöllik
Research group ROADMAP-5G, Carinthia University of Applied Sciences, Klagenfurt, Austria
e-mail: c.uran@cuas.at
URL: https://www.fh-kaernten.at/ce/

V. Egger
e-mail: v.egger@cuas.at

K. Horvath
e-mail: k.horvath@cuas.at

H. Wöllik
e-mail: h.woellik@cuas.at

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_26

1 Introduction and Background

Computer networks are ubiquitous in our modern lives. We rely on them in professional as well as private settings and mostly take this critical infrastructure for granted. As a result, unexpected network outages or their reduced performance can have very negative effects. This also includes network downtime costs and network inefficiency costs [1]. Therefore, constant network tests and performance measurements play a key role in ensuring uninterrupted availability of critical services as well as optional services which we all are used to.

It is essential that these network tests and measurements are also well documented and archived for later analysis. This includes the specifications and schedules of the tests, the Key Performance Indicators (KPIs) associated with each measurement, and the generated results. However, centralizing and storing measurement data is sometimes challenging in distributed network environments and requires the definition of intuitive and efficient interfaces [4]. Also, the generation of comprehensible reports that include all the data necessary for analyzing the issue at hand is difficult.

This paper describes the architecture and the setup of a containerized and distributed solution for measuring an arbitrary computer network's performance. The containerization of the solution facilitates rapid deployment of the different components as well as a separation of concerns, which is desired in modern software development workflows [3, 8]. The solution presented here is also able to test the network's properties against freely definable KPIs. This solution is named Automated Network Evaluation and Test Environment (ANETtE) and can be used in a wide variety of networks, such as office and enterprise networks, cellular networks, global telecommunication networks such as the Internet, as well as any combination of the aforementioned networks.

The remainder of this paper is structured as follows. Section 2 describes the setup of the environment as well as the problems that arose during the configuration and management of its components. Section 3 outlines the setup of the solution, its implementation, and usage. Section 4 discusses the reports resulting from the proposed system. Section 5 explains how the system affects the management of the research network, while Section 6 concludes the paper.

2 Problem Statement

This section describes the setup of the *5G Playground Carinthia* as well as the problems that arose during the configuration and management of its components, which eventually led to the development of ANETtE.

2.1 5G Playground Carinthia

The authors developed and tested this solution at the *5G Playground Carinthia*[1], in which a 5G research network is operated. This enables different use cases to experiment with the capabilities provided by upcoming mobile communication standards [9]. Currently, these use cases are researching the areas of autonomous drone swarms, connected robotics, smart cities, virtual realities, and fog computing. A structural overview of this research network can be seen in Fig. 1 and consists of the following parts.

Enterprise LAN This part of the *Playground* replicates a centrally managed local network infrastructure based on Cisco Meraki[2] hardware and software. It consists of multiple switches as well as two Cisco Meraki MXs, which are the union of a router, firewall, and gateway. Similar networks are commonplace in corporate settings. This network provides the use cases with the ability to connect their devices to the Internet (via the symmetric 1 Gbit/s connection). It also provides a link to the devices connected to the cellular 5G research network and the servers hosted in the Edge (see next point).

Exoscale Cloud Exoscale[3] is a European cloud hosting provider that offers compute, storage, and networking resources that are hosted in Austria, Bulgaria, Germany, and Switzerland. Additionally, the *Playground* was offered to host a small and exclusive site at the *Playground's* location in Klagenfurt. This local site is called the *Edge* and enables operating the HyperBlox 5G Core (see next point) directly on the premises of the *Playground*.

HyperBlox 5G Core According to their website,[4] "HyperBlox is pioneering a framework to make development, deployment and management of telecom applications as simple as web applications". HyperBlox provides an extensible, scalable, fully containerized, and cloud-native cellular network core. The core can run on generic hardware, which makes it ideal for the *Playground*, where it runs in the Exoscale cloud. Furthermore, the core is under active development to meet the constantly changing requirements of the use cases.

2.2 Continuous Tests and Measurements

Consistent and continuous network tests and performance measurements are important tasks in any kind of computer network, as described by Ma et al. [7] as well as Ekelin and Nilsson [5]. Especially, future cloud-, edge-, and fog-based networks are

[1] For detailed information, see https://5gplayground.at/.

[2] see https://meraki.cisco.com/.

[3] see https://www.exoscale.com/.

[4] see https://hyperblox.io/.

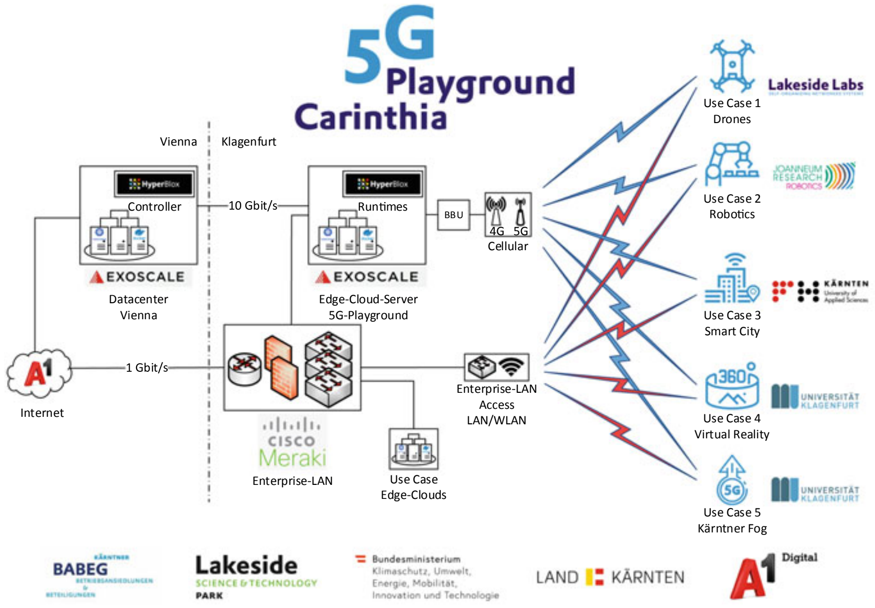


Fig. 1 Basic structure of the network inside the *5G Playground Carinthia* in Klagenfurt, Austria. It shows the symmetric 1 Gbit/s Internet connectivity, the Exoscale clouds located in Klagenfurt and Vienna, the HyperBlox 5G research core, the Enterprise LAN based on Cisco Meraki, and the five currently active use cases

characterized by a similar complexity and heterogeneity as the network described in Sect. 2.1 (see Chap. 8 in [12]). However, these properties make standardized tests and measurements challenging. Although different measurement and test software is available for various devices and their architectures, there are no standardized interfaces available between them.

This, however, would be necessary for centrally managed test and measurement procedures and their respective evaluations. It should be possible to define scheduled measurements of various network performance indicators. They should then be triggered at the desired point in time, the desired device(s), and with the desired parameters. As soon as the measurements have finished, their results should be centrally collected and being made available for analysis. In addition to customized analysis, pre-defined reports and a check of their KPIs should enable a consistent and continuous loop of measuring, testing, and reporting.

3 System Setup

As described above, a containerized architecture is desired when developing new applications. This holds especially true when said application is distributed across a heterogeneous infrastructure such as the *5G Playground Carinthia*. With containers, it is possible to package software and its dependencies together in a fast, efficient, and reproducible way. Containers make use of the functionalities provided by the Linux kernel to isolate the execution environments of different containers from each other [11]. The most popular containerization platform is Docker,[5] which is also used for the development and deployment of ANETtE. An important difference between classical virtualization and containerization is that with virtualization, each instance has its independent operating system, whereas, with containerization, the operating system kernel is shared across all instances. This makes containers more lightweight, but also less isolated [2].

Another essential point is the communication between the instances, which are running on different parts of the infrastructure. This requires well-defined interfaces between them. A widespread approach to achieve this is to use so-called *RESTful APIs*—Application Programming Interfaces adhering to the Representational State Transfer paradigm. This concept utilizes Hypertext Transfer Protocol (HTTP), including its methods and its status codes, to enable a standardized communication between the components of an application [6].

The implementation of the program logic itself has been done in *Python*[6], and the API has been realized using the Python library *FastAPI*.[7] The advantage of this concept is that Python is portable and can be containerized for different architectures. Also, FastAPI provides a boilerplate for developing and documenting APIs efficiently using integrated tools.

As can be seen in Fig. 2, ANETtE consists of four different types of containers. These, as well as how they interact with each other, are described below.

Manager The *Manager* is the central component of ANETtE. Like most of the other components, it is written in Python and uses FastAPI for implementing the RESTful API to communicate with the other components. It is used by the test engineer to manage the test specifications stored in the database. Configured and activated test specifications are read by the *Manager* and triggered accordingly. The most important configuration parameters are the schedule (either as a point in time or as `cron` syntax[8]), the type (currently, either `ping` or `iperf`), the server, the client, and the duration. As soon as the configured time has come, the measurement will be triggered on the appropriate *Worker* instance(s). Upon completion, the result(s) will be fetched from the *Worker* instance(s) and stored in the database.

[5] see https://www.docker.com/.

[6] see https://www.python.org/.

[7] see https://fastapi.tiangolo.com/.

[8] see https://crontab.guru/.

Worker The execution of the measurements is done by the *Worker* instances. This component can be instructed to perform different measurements by the *Manager* via a RESTful API. Currently, the *Worker* can act as an `iperf` server, `iperf` client, or as a `ping` client (i.e., sending ICMP echo requests and receiving ICMP echo replies) with different options. Examples for said options are the measurement duration, the used protocol (*TCP* or *UDP*) for `iperf`, and the interval or the packet size for `ping`. Furthermore, the generated results are provided to the *Manager* via the RESTful API. This is done exclusively in JavaScript Object Notation (JSON) format to eliminate the need for parsing different formats at the *Reporter* (see below) and make the subsequent evaluation easier for the test engineer.

Reporter This component is based on a modified version of *Jupyter Lab*.[9] It includes everything that is needed to read the measurement results and the KPIs from the database, perform evaluations and analyses based on them, generate documents to present the gathered information, and export these documents as Portable Document Format (PDF) files. Details on this can be found in Sect. 4 below.

MariaDB This is the only off-the-shelf component that is used inside ANETtE and provides the central database to use by all the other components.

4 Report Generation

All the gathered and stored measurement results can be evaluated using the *ANETtE Reporter*, which is a modified version of *Jupyter Lab*'s SciPy[10] Docker image. It has been modified so that it can access the *MariaDB* database out of the box. The so-called *computational notebooks* generated with *Jupyter Lab* can be used to "combine software code, computational output, explanatory text, and multimedia resources in a single document" using appropriate programming languages like *Python*, *Julia*, or *R* [10]. Because it is running on a server, it can also be used by multiple users at the same time. This makes it perfect to generate reports from stored data as is the case with *ANETtE Reporter*. There is also the possibility to freely define text cells, which can be used to write interpretations and explanations of the generated tables and plots.

In the *Reporter*, there are two distinct types of reports defined.

1. The *Overall Report* is used for displaying a summary of the measurements conducted within a given time frame. The report searches for measurements that have been conducted within the time frame and presents the relevant configuration, as well as aggregated measurement results and—if KPIs have been defined for the given specification—an evaluation of the measured data in a table. An example

[9] see https://jupyterlab.readthedocs.io/en/stable/.

[10] A set of libraries for scientific computations (see https://www.scipy.org/).

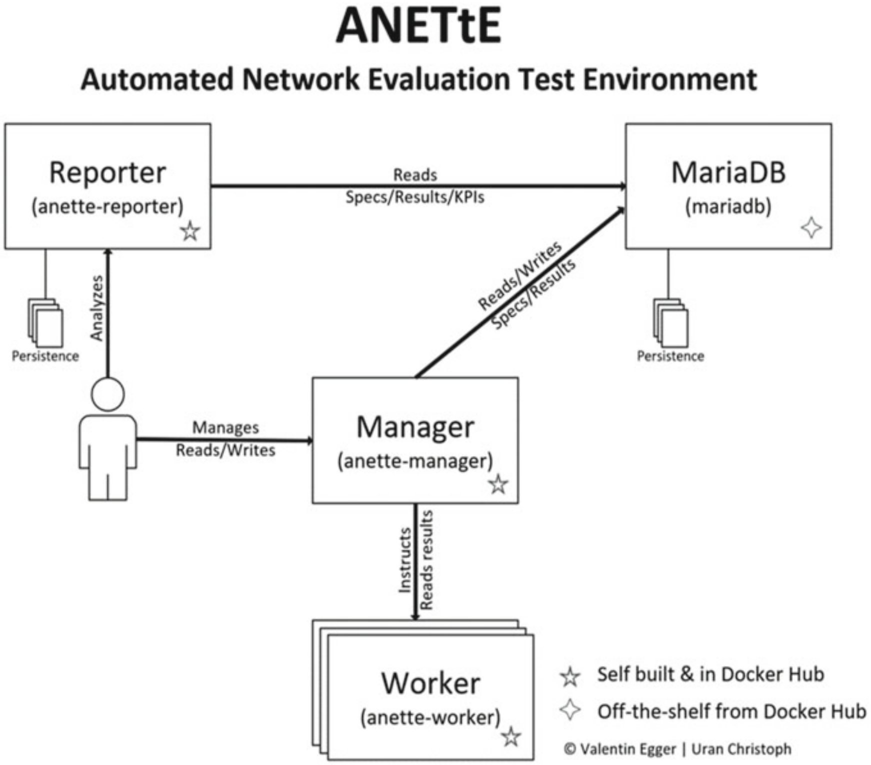
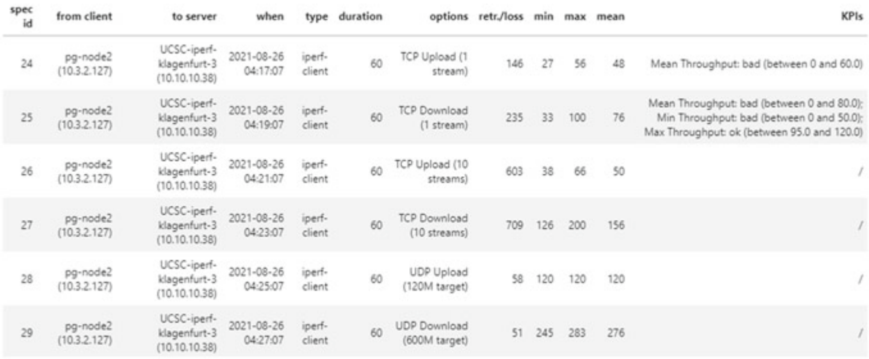


Fig. 2 Setup of the containers inside ANETtE. The *Manager* is responsible for defining and triggering measurements, as well as gathering the results and storing them. The *Worker* executes the respective measurements and provides the results. The *Reporter* is used for analyzing the results and *MariaDB* provides persistent storage

for some `iperf` measurements, that have been conducted on 08-26-2021 can be seen in Fig. 3.

2. The *Detailed Report* is used for getting detailed information about a given measurement. This includes a plot of the gathered results (both from the client- and server-side) and a tabular representation of interesting metrics of the given measurement. If KPIs for the specification of the given measurements are set, the first given KPI is used for the background coloring of the plot. Furthermore, all configured KPIs are also checked in the tabular representation. The measurement of specification ID 25 from Fig. 3 is evaluated in detail in Fig. 4.

Both of these reports can be exported to PDF files using a small `bash` script inside *Jupyter Lab*, which ensures that the code cells are not included in the PDF file, thus preventing the confusion of test engineers and decision-makers.

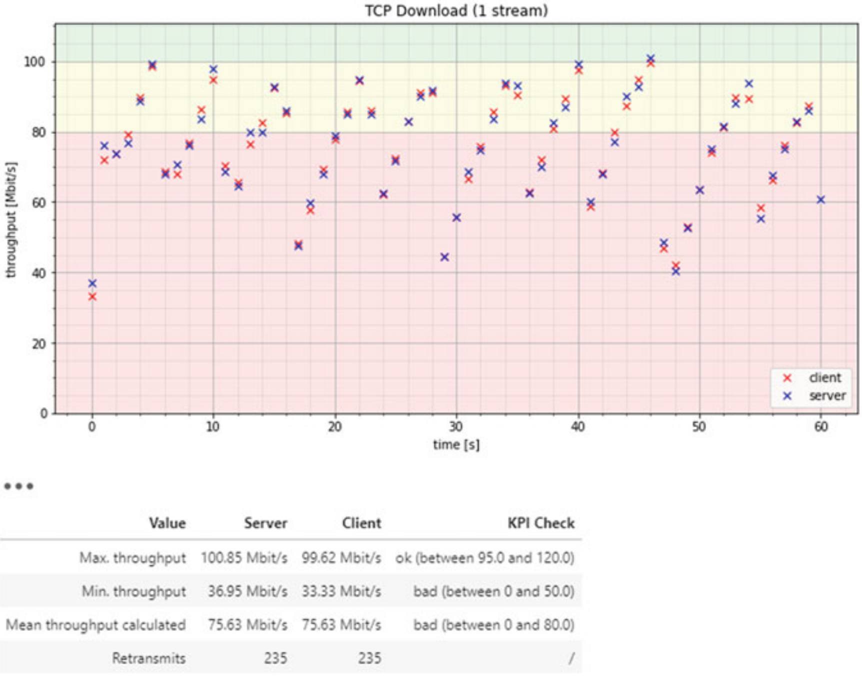


spec id	from client	to server	when	type	duration	options	retr./loss	min	max	mean	KPIs
24	pg-node2 (10.3.2.127)	UCSC-iperf-klagenfurt-3 (10.10.10.38)	2021-08-26 04:17:07	iperf-client	60	TCP Upload (1 stream)	146	27	56	48	Mean Throughput: bad (between 0 and 60.0)

25	pg-node2 (10.3.2.127)	UCSC-iperf-klagenfurt-3 (10.10.10.38)	2021-08-26 04:19:07	iperf-client	60	TCP Download (1 stream)	235	33	100	76	Mean Throughput: bad (between 0 and 80.0);
											Min Throughput: bad (between 0 and 50.0);
											Max Throughput: ok (between 95.0 and 120.0)

26	pg-node2 (10.3.2.127)	UCSC-iperf-klagenfurt-3 (10.10.10.38)	2021-08-26 04:21:07	iperf-client	60	TCP Upload (10 streams)	603	38	66	50	/
27	pg-node2 (10.3.2.127)	UCSC-iperf-klagenfurt-3 (10.10.10.38)	2021-08-26 04:23:07	iperf-client	60	TCP Download (10 streams)	709	126	200	156	/
28	pg-node2 (10.3.2.127)	UCSC-iperf-klagenfurt-3 (10.10.10.38)	2021-08-26 04:25:07	iperf-client	60	UDP Upload (120M target)	58	120	120	120	/
29	pg-node2 (10.3.2.127)	UCSC-iperf-klagenfurt-3 (10.10.10.38)	2021-08-26 04:27:07	iperf-client	60	UDP Download (600M target)	51	245	283	276	/

Fig. 3 Tabular representation of active measurement specifications including their results and the evaluation of the respective KPIs in a given time frame



Value	Server	Client	KPI Check
Max. throughput	100.85 Mbit/s	99.62 Mbit/s	ok (between 95.0 and 120.0)
Min. throughput	36.95 Mbit/s	33.33 Mbit/s	bad (between 0 and 50.0)
Mean throughput calculated	75.63 Mbit/s	75.63 Mbit/s	bad (between 0 and 80.0)
Retransmits	235	235	/

Fig. 4 Detailed representation of the measurement of specification ID 25 from Fig. 3. It includes a plot and a detailed analysis according to the KPIs.

5 Results

Inside the *5G Playground Carinthia*, the whole ANETtE system and the resulting reports are used by the test engineers regularly. The reports are primarily used for documentation and as a prove for contractors as well as the use case owners (as described in Sect. 2.1). On the contractor side, the test engineer needs regular and reproducible measurements and tests to hold each contractor accountable for their part of the network. Toward the use case owners, it is important to have documented proof of the performance that selected parts of the network were able to achieve at a given point in time.

Before the adoption of ANETtE, all relevant measurements and tests had to be initiated, documented, and analyzed manually. This resulted in a significant workload on top of the usual work of the administrators of the *Playground*. Furthermore, no raw data was collected during the old measurement procedure. The interpretation was done by the administrators directly upon seeing the results and documented inside a central Excel sheet. Due to the lack of raw data, no full historical comparison of the measurements was possible. This issue has now been fixed, and a full historical performance comparison is possible at any time.

6 Discussion and Conclusion

Permanently measuring and testing the performance of the different components involved in a heterogeneous telecommunication network such as the *5G Playground Carinthia* is a challenging task. Usually, test engineers or administrators have to conduct, document, and analyze the measurements manually, which leads to a significantly increased workload and also increases the likelihood of errors. Therefore, ANETtE introduces an automated, distributed, and fully containerized way to specify, store, document, and report on measurements of relevant parameters in a telecommunication network. The containerization increases portability, scalability, and modularity and promotes standardized communication between the components using well-defined interfaces. The generated reports can be used for documentation as well as decision-making support for the different parties involved in the management and the utilization of the network.

ANETtE is still under active development, and there are some optimizations to be done as well as some stability issues in the *Worker* that need to be fixed. Most of them are related to the measurement processes not exiting correctly. Furthermore, additional helper functions will be defined for the *Reporter* in addition to the existing ones for database access. This includes helper functions for statistical data analysis, plotting, and other areas.

The Docker images are available to download and use from Docker Hub.[11] It is planned to eventually license the whole system using an open-source license and to publish the source code. This should encourage the adoption and create an ecosystem around it, making it easier to improve the system.

References

1. Angrisani L, Narduzzi C (2008) IEEE Instrum Measure Mag. Testing communication and computer networks: an overview 11(5):12–24
2. Bhatia G, Choudhary A, Gupta V (2017) The road to docker: a survey. Int J Adv Res Comput Sci 8(8)
3. Burns B, Oppenheimer D (2016) Design patterns for container-based distributed systems. In: 8th {USENIX} workshop on hot topics in cloud computing (HotCloud 16)
4. Cecchinel C, Jimenez M, Mosser S, Riveill M (2014) An architecture to support the collection of big data in the internet of things. In: 2014 IEEE world congress on services, pp 442–449. IEEE
5. Ekelin S, Nilsson M (2004) Continuous monitoring of available bandwidth over a network path. In: Proceedings of 2nd Swedish national computer networking workshop (SNCNW 2004)
6. Fielding RT (2000) Architectural styles and the design of network-based software architectures. University of California, Irvine
7. Ma L, Li X, Su Z (2014) A method for discretization of continuous attributes in network performance measurement. In: 2014 IEEE workshop on electronics, computer and applications. pp 88–91. IEEE
8. Mili H.,Elkharraz A, Mcheick H (2004) Understanding separation of concerns. Early aspects: aspect-oriented requirements engineering and architecture design, pp 75–84
9. Navarro-Ortiz J, Romero-Diaz P, Sendra S, Ameigeiras P, Ramos-Munoz JJ, Lopez-Soler JM (2020) IEEE Commun Surv Tutor. A survey on 5g usage scenarios and traffic models 22(2):905–929
10. Perkel JM (2018) Nature. Why Jupyter is data scientists' computational notebook of choice 563(7732):145–147
11. Plauth M, Feinbube L, Polze A (2017) A performance survey of lightweight virtualization techniques. In: European conference on service-oriented and cloud computing, pp 34–48. Springer
12. Sunyaev A, Sunyaev A (2020) Internet computing. Springer

[11] see https://hub.docker.com/u/cuas5g.

A Security and Privacy-Preserving Accessing Data Protocol in Vehicular Crowdsensing Using Blockchain

Abdulrahman Alamer and Sultan Basudan

Abstract This paper exploits the advantage of blockchain to fulfill secure data storage and access in vehicular crowdsensing. In vehicular crowdsensing, organizations can have a right to access vehicles' profiles with unlimited privilege, which results in security and privacy disclosure. Thus, based on the proposed blockchain, we design a secure and privacy-preserving vehicle's profile record accessing (BSPPA) protocol. The proposed BSPPA is able to store the vehicle's sensing data and indexes as encrypted data for a secure indexes search. This will result in controlling the privilege of data access and prevent vehicle's data from being revealing private data. Analysis of the security is demonstrated to show the efficiency of the BSPPA scheme. Furthermore, the performance evaluation shows the efficiency of the BSPPA protocol.

Keywords Smart vehicle · Sensing data · Vehicular crowdsensing · Blockchain · Security and privacy-preserving

1 Introduction

Nowadays, modern vehicles are equipped with various of sensor devices and wireless communication devices that are controlled by an internal onboard unit (OBU) [10, 16]. It is conceived that vehicle is able to collect several different types of sensing data that can be utilized to provide multiple applications, such as road conditions, weather conditions, and health conditions [17]. In a vehicular crowdsensing (VCS) system, the vast number of intelligent vehicles is encouraged to participate by their resources sensing data to supply different vehicular applications [1]. The key role of the VCS paradigm is to allow an organization who is responsible to administrate a particular vehicular application to generate a vehicular task $t_{\in}T$ in order to obtain an specific

A. Alamer (✉) · S. Basudan
Department of Information Technology and Security, Jazan University, Jazan, Saudi Arabia
e-mail: amalameer@jazanu.edu.sa

S. Basudan
e-mail: sbasudan@jazanu.edu.sa

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_27

sensing data for supplying its application [11]. For example, the organization og_i will send a task t_i to the VCS-server. Thus, the VCS-server will recruit the suitable vehicle i to perform the t_i. Note that, vehicle i can be recruited to participate in number n of vehicular tasks $(t_i)_{i=1}^{n}$. Thus, vehicle i will perform different tasks $(t_i)_{i=1}^{n}$ and sends the corresponding results to the VCS-server. The vehicle will participate on the announcement task t_i and sends the results back to the VCS-server. Once received the results, the VCS-server will store it in the vehicle i's profile record. Finally, each organization og_i can then access to the vehicle i's profile to collect their requested sensing data [18].

Nevertheless, the successful of vehicular applications is based on the information that must be collected from vehicles' sensor devices [2]. However, without existing of any security strict on preventing the accessing a vehicle's profile records, this will significantly make both vehicles and organizations private information under the violation issues. Consider the following scenario, if a vehicle i is recruited to participate in two different vehicular tasks (t_1, t_2) for two different organizations (og_1, og_2). If the organization (og_1) obtains access to the vehicle i' profile record for collecting the sensing data result of task (t_1), it can also reach the vehicle i' private data as well as to the sensing data of the task (t_2) that is intended for organization (og_2). Therefore, security and privacy issues are essential to the VCS applications success. Specifically, the vehicles' profile record in VCS-server must be protected from unauthorized accessing [13]. Otherwise, it will be impossible to encourage vehicles to participate in vehicular tasks.

According to the vehicles' privacy issues, many works have been done to protect the participated vehicles' sensing data from being disclosed [19, 21, 23]. However, these works are concentrated on protecting content of sensing data during their transmission journeys, which are from vehicles-to-fog node and from fog node-to-VCS-server [5]. In contrast, protecting vehicle's profile record from unauthorized accessing by different organizations seem to be ignored. In the fact, without any security policies on accessing vehicle's profile record, malicious organization can easily disclose vehicle's private data as well as other organization's request data. So as to perfectly secure the vehicle's profile record in VCS system, it is essential to purpose a secure scheme for restricting the access to the vehicle's profile record.

To perfectly solve the above-mentioned issues, blockchain technology is proposed in order to tackle the aforementioned security issues inherited in VCS-server accessing system [20, 27]. Essentially, blockchain is utilized to store crowdsensing data as blocks for distributing data access. Although blockchain has advantages of immunity, distribution, and safe accessing system, blockchain-based VCS accessing system still faces some challenges. The first concern is in how to design a blockchain mechanism with a feature of verifying and accessing vehicle's profile without violating the vehicle's private data. The second challenge is how to ensure that each authorized organization has a limit privilege access to the intended data. One more concern is how to ensure that unauthorized or even authorized organization cannot be able to access or link a different sensing data report that is intended to the other organization.

Motivated by the above challenges, we encourage to design a secure and privacy-preserving based on a blockchain technology to protect vehicle's profile record from unauthorized access by the organizations. The paper contributions are threefold.

- We propose a blockchain-based framework for VCS accessing with security and privacy preservation for improving organizations applications in VCS system. The blockchain stores the original vehicle's sensing reports, which are encrypted for security.
- Based on the blockchains mechanism [30], we design a blockchain mechanism with fundamental components to be compatible with VSC system, including data structure and access mechanism. The VSC blockchains are referred as a VCS-BC.
- Based on the elliptic curve cryptography (ECC) public encryption method [11], we propose a secure and privacy-preserving vehicle's profile record accessing (BSPPA) protocol for the proposed VCS-BC. The BSPPA scheme will encrypt the vehicle's sensing data with the identical keywords for a achieving data security. The BSPPA scheme is designed for a carefully ensure that only the authorized organization with a valid permission to access the interested sensing data.

The remainder of the paper is organized as follows. An overview on the related work is conducted in Sect. 2. Section 3 illustrates the system model, the threat model, and design goals of the work. Preliminaries are presented in Sect. 4. Section 4.2 presents the proposed BSPPA protocol in details. We provide security analysis in Sect. 5 and performance evaluation in Sect. 6. Finally, Sect. 7 concludes the paper.

2 Related Work

Because vehicle is rated as an accurate entity to provide various sensing data, many works have designed incentive mechanism to stimulate vehicles to participate in the VCS announcement tasks [22, 28]. In addition, many security schemes have been proposed in order to protect vehicles private data during their participating for encourage vehicles to send their data with full guarantee of protecting their privacy from any malicious attacks [7, 8, 29]. However, these schemes still suffer from guarantee of protecting vehicle's privacy from accessing the vehicle's profile records from the organization requester. Therefore, to address these issues regarding to accessing vehicle's record, the blockchain technology can be exploited for prevent vehicle's profile record from unauthorized accessing. Recently, blockchain technology has attracted growing attention and research work in the context of vehicular networks due to its characteristics of decentralization, anonymity, and trust [24]. Blockchain can help establishing a secure, trusted, and decentralized intelligent transport system, thus address data accessing problems to provide a full guarantee of security on the storages sensing data [25, 26] . However, these works do not give a detail solution for a specific application. In this work, we design a security and private-preserving accessing (BSPPA) protocol for the proposed VCS-BC system.

3 System Model and Design Goals

This section describes the system model for the VCS system based on the proposed BSPPA protocol. Then, we present the threat model and design goals.

3.1 System Model

As illustrated in Fig. 1, the system is mainly composed of the following entities:

- Organizations: Each organization has an authorized vehicular application, and it can release VCS tasks in order to obtain sufficient resources data from vehicles to support its vehicular application.
- Vehicular crowdsensing (VCS) servers: The VCS-server has enormous capabilities for storage and computational. In addition, it is responsible to announce VCS tasks that are released by organizations for all connected vehicles. At the same time, it is responsible to recruit suitable vehicles for that announce VCS tasks and then stores the vehicles sensing reports in the proposed VCS-BC.
- Smart vehicles: Each smart vehicle is equipped with various sensors and a powerful OBU. A vehicle can be required to participate in more than two VCS tasks [6]. The required vehicle should perform the task and sends the results to the VCS-server as encrypted data.
- Roadside unit (RSU): The RSU acts as a gateway between the VCS-server and vehicles. It is responsible to deliver the messages from the VCS-server to vehicles as well as it collects and transmits all the related information of the involved vehicles to the VCS-server [4, 12].
- Trust authority (TA): It charges the whole system. All the organizations, RSUs, and vehicles are required to register with the system manager. It generates system parameters and public and private keys for each registered entity.

3.2 Security Threat Model

Accessing vehicle's profile record by number of organizations is considered as the main security threats in this work. When a vehicle accepts to participate to sense data for different organizations. It will definitely have concerns for its sensitive data that may be accessed by these organizations [14]. Assume this vehicle senses weather data in particular location that should be supported for an organization that is responsible to administrate a weather application. Thus, if other organizations have also accessed to the same vehicle's profile record to collect its intended sensing data, it can disclose the vehicle's location as well as it can disclose the private sensing data to the organization who is responsible to administrate a weather application. In addition, we assume RSUs and VCS-server are deemed as semi-trusted. They are honest to perform the protocol but curious to access or deduce the vehicles' or organizations'

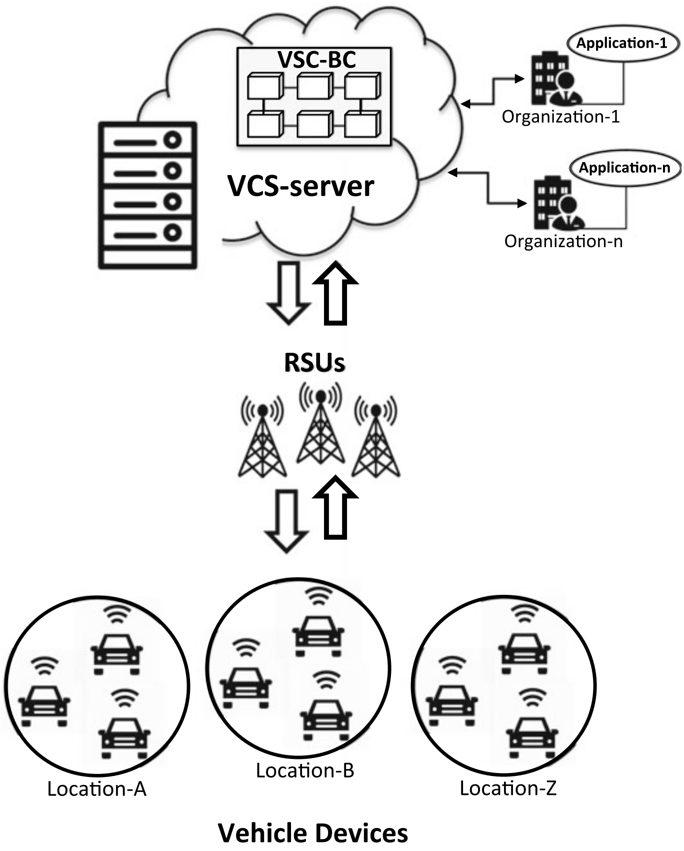


Fig. 1 VCS-BC system model

information without authorization. Thus, the vehicle and organizations privacy is under security threats. For avoiding the security and privacy issues, we have adopted the blockchain technology [30] to design a compatible VSC blockchain (VCS-BC) system. In addition, we adopt the ECC public encryption method [11] to design a secure and privacy-preserving vehicle's profile record accessing (BSPPA) protocol for the proposed VCS-BC system.

3.3 Design Goals

The paper goals are to achieve the following security features:

- **Confidentiality and integrity**. Since announcement tasks and sensing reports are type of sensitive data, data confidentiality and integrity are critical to be achieved.

- **Secure data access**. Since vehicle's profile include sensitive data, access control is critical to be achieved. The authorized organization only is allowed to obtain a limited privilege access without disclosing vehicle's privacy.
- **Secure search**. Since vehicle's profile include different sensitive data that are related to different organization, the secure search is critical to be achieved. Only the authorized organization that possesses a sensing data stored in the vehicle's profile can obtain a valid key by a vehicle and VCS-server to search for its sensing data.

4 The BSPPA Protocol

4.1 Preliminaries

This subsection will present the main preliminaries that are required for achieving the proposed BSPPA scheme.

1) **Blockchain mechanism** The blockchain is a database that is format as a list of blocks connected together [15]. In this work, we design a secure accessing data for VCS system based on the blockchain mechanism referred as VCS-BC. In the proposed VCS-BC, the VCS-server is responsible to manage the access right to a vehicle's profile record, which only the organization with a permission key is allowed to access on a particular block in the VCS-BC. Each block in the VCS-BC consists of a block header, payload, and backside, as described below:
    - The block header consists of two components: Block identity and hash value of previous block.
    - The block payload consists of four components: Task identity, vehicle's pseudo-identity, encrypted sensing data, and secure keyword.
    - The block backside consists of two components: Contributors signatures that are used to track the participated vehicle and VCS-server, and timestamp of the block that shows the generation time.
2) **Bilinear maps** Let G_1 and G_2 are two multiplicative cyclic groups with the same prime order q. A bilinear mapping $\hat{e} : G \times G \rightarrow G_T$ is an admissibility properties with satisfying the following properties:
    - Bilinearity: $\forall g, v \in G_1$ and $a, b \in Z_q^*$, $\hat{e}(g^a, v^b) = \hat{e}(g, v)^{ab} = \hat{e}(g_1^b, g_2^a)$.
    - Non-Degeneracy: $\hat{e}(g, v) \neq 1_{G_2}$.
    - Admissibility: $\hat{e}(g, v)$ is efficiently computable.
3) **Complexity assumption** The intractable mathematical problem and complexity assumption used are as follows. **q-Decisional Bilinear Diffie–Hellman (q-DBDH)**. Given $g, g^a, g^b, g^c \in \mathbb{G}_1,\ \forall a, b, c \in Z_q^*$, the q-DBDH problem is to decide whether $f = \hat{e}(g, g)^{abc}$, where $f \in \mathbb{G}_2$. **Definition 1**. An algorithm $\Im$

with an output $\beta \in \{0, 1\}$ has an advantage ε in solving the q-DBDH problem that

$$| \Pr[\Im(g, g^a, g^b, v, \hat{e}(g, v)^{ab}) = 1] - \Pr[\Im(g, g^a, g^b, v, z) = 1] | \geq \varepsilon$$

where $a, b \in Z_q^*$ and $z \in G_2$. The (ι, ε)-q-DBDH assumption holds if no $\Im$ algorithm with an advantage ε and running time ι to solve the q-DBDH problem.

4.2 The Detailed BSPPA

To achieve security and privacy-preserving accessing data in VCS system, we utilize the blockchain and ECC public key to design the secure access method matching in VCS system. We allow each organization to obtain their requested sensing data from the participated vehicle's profile record without revealing the vehicle's privacy. The ECC public encryption method [11] is used to fulfill the privacy search for intended block in the proposed blockchain. Specifically, the vehicle's sensing data is stored in a block with a linked keyword as an index for the block. Thus, the organization can find the intended block with no knowledge about other block. The detailed construction of BSPPA is described below.

1) **System setup** The TA implements this step to compute the public system parameter P_p. It choose two multiplicative bilinear groups G_1 and G_2 of prime order q, g is a generator of G_1 and $\hat{e}$ is a bilinear map: $\hat{e} : G_1 \times G_1 \rightarrow G_2$. The TA picks $\mathcal{H}$ as a collision resistant hash function as well as $C = E_{AES}(K, M)$ and $M = D_{AES}(K, C)$ as the encryption and decryption algorithm [11]. The public parameter is $P_p = \{q, G_1, G_2, \hat{e}, g, \mathcal{H}\}$.
2) **Key generation** All the system model entities are required to register to the TA. Each entity device including vehicles, VCS-server, and organizations should send their identity Id_i to the TA who will generate the following:

   - Pseudo-identity. For each device such as a vehicle i, the TA computes $pid_i = \mathcal{H}(Id_i || s_i)$ as a pseudo-identity to protect the vehicle's identity from the rainbow table attack [7] [3].
   - Public and private keys. The TA chooses a random number $x_i \rightarrow Z_q^*$ as a vehicle i's private key (sk_i) and computes $pk_i = g_i^x$ as the corresponding public key(pk_i).

   The TA then sends (pk_i, sk_i, pid_i) to the vehicle i.
3) **Releasing VCS task** If any organization og_i needs resources for its vehicular application from a particular region, it will generate an spatial task $t_i = (tid_i, cr_i, ex_i, l_i, b_i)$, which indicate the task's identity, content requirement (what to sense), the period time (when to start and end), the particular interest location (where to sense) and task benefits (compensation of task). The og_i will then send t_i to the VCS-server as an encrypted message $\delta_i(t_i)$, where δ_i is an encryp-

tion method in [9]. After receiving the $\delta_i(t_i)$, the og_i will pick a random number $\eta_i \in Z_q^*$ as a identifier of task t_i and then announces the $(\delta_i(t_i), \eta_i)$to all connected vehicles and recruit trusted vehicle i to perform the task t_i.

4) **Generating sensing data** Once the interested vehicle i received the $\delta_i(t_i)$, it will extract the task t_i and starts performing the task t_i by generating the sensing data (sd_i) according to the content requirements in cr_i. Notes that vehicle i can participate in one or more VCS tasks $t_i \in T$. To prevent the generated of the generated sensing data (sd_i), vehicle i generates a ciphertext of (sd_i) utilizes organization's public key pk_{og_i} to encrypt (sd_i). It picks a random value $r_i^1 \in Z_q^*$ as well as picks a mutual secret keyword $w_i \in Z_q^*$. It then computes $E_0 = E_{AES}[(tid_i, pk_{og_i}^{w_i r_i^1}), sd_i]$, $E_1 = P^{r_i^1}$ and $E_2 = (E_0 \cdot E_1)^{w_i x_i}$. After that, vehicle i utilizes the VCS-server' public key pk_{vcs} to encrypt the mutual secret key w_i by randomly choosing $r_i^2 \in Z_q^*$ to compute $E_3 = E_{AES}[(\eta_i, pid_i, pid_{og_i}, pk_{vcs}^{r_i^2}), w_i]$ and $E_4 = P^{r_i^2}$. Finally, vehicle i sends the encrypted sensing data $\tau_i = (\eta_i, pid_i, pid_{og_i}, E_0, E_1, E_2, E_3, E_4)$ to the VCS-server.

5) **Storging sensing data** When the VCS-server receives the ciphertext τ_i message, it will utilize its secret key x_{vcs} in order to obtain the mutual secret key w_i by decrypting E_3 as $w_i = D_{AES}[(\eta_i, pid_i, pid_{og}, E_4^{x_{vc}}), E_3]$. The VCS-server will then generate the block index keyword search by utilizing the mutual secret key w_i and a random value $z_i \in Z_q^*$ to compute $(K_0, K_1) = (P^{w_i z_i}, (E_2 \cdot pk_{og_i}^{w_i z_i})^{x_{vcs}}$. Consequently, the VCS-server will generate a new transaction to store $(\eta_i, pid_i, E_0, E_2, K_0, K_1)$ in a new block $\mathbb{B}_i$ in the proposed VCS-BC.

6) **Generating trapdoors** The VCS-server will generate two trapdoors for a keyword search and keyword encrypted sensing data, that is, $K_4 = (K_2, K_3) = (pk_{og_i}^{w_i z_i}, E_1^{w_i})$. The VCS-server will then utilize the organization public key pk_{og_i} to encrypt the trapdoors keywords as $K_5 = P^{z_i}$ and $K_6 = E_{AES}[(H_1(\eta_i), pk_{og_i}^{z_i}), K_4]$. Finally, VCS-server sends (K_5, K_6, E_0) to the organization og_i.

7) **Accessing sensing data** When the organization og_i receives the (K_5, K_6, E_0) message, it will utilize its private key x_{og_i} to decrypt K_6 in order to obtain the trapdoors keywords as, $K_4 = D_{AES}(\eta_i, K_5^{x_{og_i}}), K_6]$. With $K_4 = (K_2, K_3)$, organization og_i can obtain the block index keyword search K_0 by computing $K_0 = K_2^{-x_{og_i}}$. Consequently, organization og_i uses the K_0 to locate the intended block $\mathbb{B}_i$ in VCS-BC. It then can access to the block's payload to extract the encrypted sensing data E_0. Finally, the organization og_i recovers the original plaintext (sd_i) by decrypting E_0 using its private key x_{og_i}, such that, $sd_i = D_{AES}[(tid_i, K_3^{x_{og_i}}, E_0]$.

5 Security Analysis

In this section, we analyze how the proposed BSPPA protocol can effectively meet with the design goals.

- **The BSPPA achieves secure search** The sensing data sd_i that is generated for the task t_i is stored in the proposed VCS-BC blockchain as a ciphertext. Only the authenticated organization og_i who releases the task t_i is allowed to obtain the block index keyword search K_0 and access to the $\mathbb{B}_i$. It is impossible for a malicious organization og_j to locate the block $\mathbb{B}_i$ in VCS-BC, without known the organization og_i's private key x_{og_i} in order to obtain the encrypted trapdoor keyword K_2 and then the block index keyword search K_0. This keyword trapdoor K_2 is computed under the organization og_i public key.
- **The BSPPA achieves confidentiality and integrity** The proposed BSPPA protocol achieves data confidentiality and integrity. The sensing data sd_i is encrypted under the organization og_i public key. Thus, it is impossible for a malicious organization og_j to reveal the original plaintext of the sensing data sd_i from the $\mathbb{B}_i$' payload without known the keyword trapdoors $K_4 = (K_2, K_3)$ and the organization og_i's private key x_{og_i}. Thus, using signature method in each generated block $\mathbb{B}_i$ is critical to achieve data integrity. By this method, the proposed BSPPA protocol guarantees the data confidentiality and integrity.
- **The BSPPA achieves security of access data** A part from data confidentiality and integrity, the encrypted sensing data sd_i is not only encrypted under the organization og_i public key, it is also encrypted with a random number $r_i^1 \in Z_q^*$, a mutual secret keyword $w_i \in Z_q^*$ and the task identity tid_i. This will prevent any a malicious organization og_j to reveal the vehicle i's private data or even reveal different flows of sensing data that is generated by the same vehicle i for other organization og_k. Thus, only the authorized organization og_i who releases the task t_i with tid_i is just allowed to obtain sd_i by decrypt the $sd_i = D_{AES}[(tid_i, K_3^{x_{og_i}}, E_0]$ using its private key x_{og_i}.

6 Performance Evaluation

In this evaluation, the Hyperledger[1] platform is used to design the proposed blockchain method. The performance evaluation is operated on a laptop with i7-6700 Intel Core @3.40 GHZ, 4 GB RAM. The cryptographic primitives are executed on the MIRACL library with Weil pairing method to generate the bilinear pairing operation. The pairing is implemented on the elliptic curve that is defined as $y = x^3 + x$ over $\mathbb{F}_q$.

6.1 Evaluation of cryptographic in the BSPPA

The cryptographic algorithm that is used in the proposed BSPPA protocol is evaluated in terms of recording the computational cost of the algorithm. The computational cost of the proposed BSPPA protocol is evaluated by counting the cryptographic

[1] https://www.hyperledger.org.

operations, which are scalar multiplication in G_1, multiplication in G_2, the exponentiation in G_2 and the bilinear pairing in $\hat{e}$. We symbolize sm_{G_1}, sm_{G_2}, ex_{G_2} and $bp_{\hat{e}}$ for the point multiplication in G_1, multiplication in G_2, the exponentiation in Z_q^* and the pairing computation in $\hat{e}$. The number of complicate cryptographic operations is evaluated in each phase in the proposed BSPPA protocol. In first phase, each vehicle i computes $5sm_{G_1}$ for encrypting sensing data. Second, a VCS-server computes $7sm_{G_1}$ for generating two keyword trapdoors. Finally, the end-organization computes $3sm_{G_1}$ for decrypting the ciphertext.

1) **Evaluation storage block in the VCS-BC** The proposed BCS-BC storage cost is affected by the increasing number of storing blocks as well as the size of each storage block $\mathbb{B}_i$. Here, we will evaluate the storage overhead of each block $\mathbb{B}_i$. The VCS-server generates a transaction and stores it as a block $\mathbb{B}_i$ in the VCS-BC. The maximum size of a block $\mathbb{B}_i$ in the VCS-BC is 4 bytes. Lets $|G_1|$ and $|G_2|$ the length size of an point in G_1 and G_2, respectively, $|Z|$ the length size of an element in Z_p^* and $|M|$ the size of an element in $\{1, 0\}$. The system parameter $\kappa = 128$, the lengths of $Z_p^* = 256$ bits, $\{1, 0\} = 1024$, $G_1 = 512$ bits and $G_T = 1024$ bits. Under these settings, the storage overhead of each block $\mathbb{B}_i$ in the VCS-BC is $2|Z| + |M| + 4|G_1| = 3584$ bits. Thus, the overall size of the blockchain is calculated by the number of the blocks $n * 3584$ bits, which is increased by increasing the task number.
2) **Evaluation of communication cost in the BSPPA** According to the lengths of $|G_1|$, $|G_2|$, $|Z|$, and $|M|$, we analyze the communication overhead of proposed BSPPA protocol for each communication phases. First, vehicle i sends ciphertext $\tau_i = (\eta_i, pid_i, pid_{og_i}, E_0, E_1, E_2, E_3, E_4)$ to the VCS-server with the lengths of $3|Z| + |M| + 4|G_1|$ that is equal 3840 bits. Then, VCS-server sends (K_5, K_6, E_0) trapdoors of keyword to the end-organization with the lengths to $2|M| + |G_1|$ that is equal 2560 bits.
3) **Implement simulation of the VCS-BC** Based on the above evaluation, we implement the simulation on the hyperledger platform by setting 50 of vehicles and 3 of organizations. Each organization og_i is responsible to admin one vehicular application. In addition, a VCS-server and a RSU are setting. All setting entities are implemented on Ubuntu 16.04 operating system on virtual software. Therefore, we can find out that the storage cost of BSPPA is increased with increasing the number of selected participated vehicles in a single task t_i. In addition, the BSPPA's cost is increased when every organization release more than one task $(t_i)_{i=1}^k$ and for each $t_i \in k$ organization require to recruit k number of participated vehicles $(i)_{i=1}^k$. As shown in Fig. 2, we evaluate the rate of VCS-BC storage when the number of tasks is equal to the number of participated vehicles. In contrast, in Fig. 3, we evaluate the rate of VCS-BC storage when the number of participated vehicles is double of the number of tasks, which means that an organization requires two vehicles to participate in a task. Thus, the storage cost of BSPPA is increased with increasing the number of announcement tasks and number of participated vehicles.

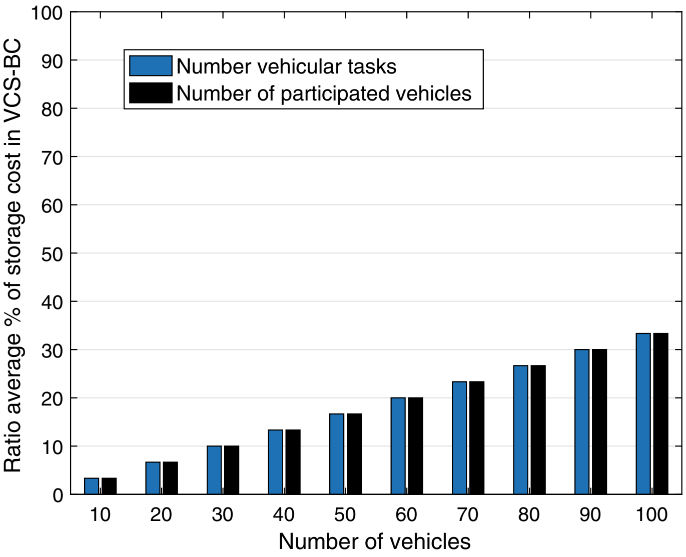


Fig. 2 Number of tasks is equal to the number of participated vehicles

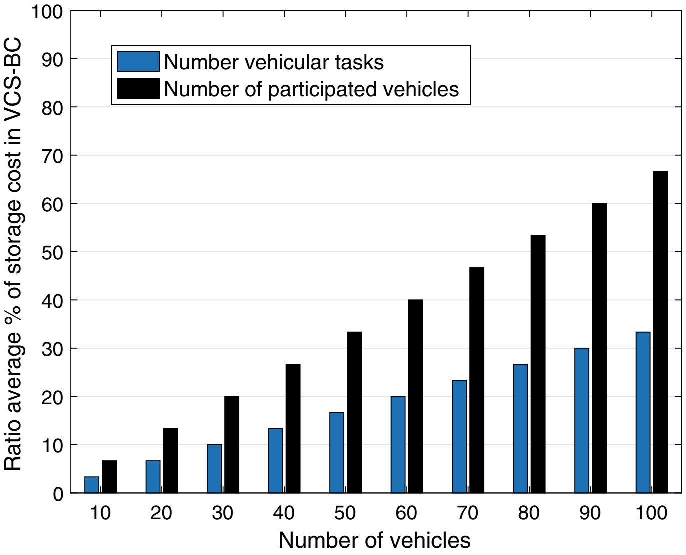


Fig. 3 Number of participated vehicles is double of the number of tasks

7 Conclusion

This paper exploits the blockchain technology to design a security and privacy blockchain in VCS system to protect vehicle's profile record from multiple accesses by organizations. First we designed blockchain that is compatible with storage record system in the VCS-server. The designed VCS-blockchain is referred as VCS-BC. In addition, we exploit the elliptic curve cryptography (ECC) public encryption method to propose a secure and privacy-preserving vehicle's profile record accessing (BSPPA) protocol for the designed VCS-BC system. The proposed BSPPA protocol is able to store the vehicle's sensing data and indexes as encrypted data in order to achieve data security, access control, privacy preservation, and secure indexes search. Security analysis demonstrates that the proposed protocol meets all the security goals. Furthermore, the performance evaluation shows the efficiency of the BSPPA protocol. Future work will focus on an in-depth study of the security and privacy-preserving issues related to guaranteeing the privacy of Internet of things (IoT) applications in VCS system.

References

1. Abdelrahman A, El-Wakeel AS, Noureldin A, Hassanein HS (2020) IEEE Netw. Crowdsensing-based personalized dynamic route planning for smart vehicles 34(3):216–223
2. Alamer A (2020) An efficient group signcryption scheme supporting batch verification for securing transmitted data in the internet of things. J Ambient Intell Hum Comput 1–18
3. Alamer A (2020) A secure anonymous tracing fog-assisted method for the internet of robotic things. Library Hi Tech
4. Alamer A (2021) Security and privacy-awareness in a software-defined fog computing network for the internet of things. Opt Switch Netw 100616
5. Alamer A, Basudan S (2020) An efficient truthfulness privacy-preserving tendering framework for vehicular fog computing. Eng Appl Artif Intell 91:103,583
6. Alamer A, Basudan S, Hung PC (2020) A secure tracing method in fog computing network for the iot devices. In: Proceedings of the 12th international conference on management of digital ecoSystems, pp 104–110
7. Alamer A, Basudan S, Lin X (2018) A privacy-preserving incentive framework for the vehicular cloud. In: 2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). IEEE, pp 435–441
8. Alamer A, Deng Y, Lin X (2017) A privacy-preserving and truthful tendering framework for vehicle cloud computing. In: 2017 IEEE international conference on communications (ICC). IEEE, pp 1–7
9. Alamer A, Deng Y, Lin X (2017) Secure and privacy-preserving task announcement in vehicular cloud. In: 2017 9th International conference on wireless communications and signal processing (WCSP). IEEE, pp 1–6
10. Alamer A, Deng Y, Wei G, Lin X (2018) IEEE Netw. Collaborative security in vehicular cloud computing: a game theoretic view 32(3):72–77
11. Alamer A, Ni J, Lin X, Shen X (2017) Location privacy-aware task recommendation for spatial crowdsourcing. In: 2017 9th International conference on wireless communications and signal processing (WCSP). IEEE, pp 1–6

12. Basudan S (2020) J Commun Inf Netw. LEGA: a lightweight and efficient group authentication protocol for massive machine type communication in 5g networks 5(4):457–466
13. Basudan S (2021) A puncturable attribute-based data sharing scheme for the internet of medical robotic things. Library Hi Tech
14. Basudan S, Alamer A, Lin X, Sankaranarayanan K (2018) Efficient deduplicated reporting in fog-assisted vehicular crowdsensing. In: 2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE Smart data (SmartData). IEEE, pp 463–469
15. Bodkhe U, Tanwar S, Parekh K, Khanpara P, Tyagi S, Kumar N, Alazab M (2020) Blockchain for industry 4.0: A comprehensive review. IEEE Access 8:79,764–79,800
16. Ho TM, Tran TD, Nguyen TT, Kazmi S, Le LB, Hong CS, Hanzo L (2019) Next-generation wireless solutions for the smart factory, smart vehicles, the smart grid and smart cities. arXiv:1907.10102
17. Ji B, Zhang X, Mumtaz S, Han C, Li C, Wen H, Wang D (2020) IEEE Commun Stand Mag. Survey on the internet of vehicles: network architectures and applications 4(1):34–41
18. Le DT, Kaddoum G (2021) LSTM-based channel access scheme for vehicles in cognitive vehicular networks with multi-agent settings. IEEE Trans Veh Technol
19. Li H, Han D, Tang M (2020) A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing. IEEE Syst J
20. Lin X, Wu J, Mumtaz S, Garg S. Li J, Guizani M (2020) Blockchain-based on-demand computing resource trading in IOV-assisted smart city. IEEE Trans Emerg Top Comput
21. Masood A, Lakew DS, Cho S (2020) IEEE Commun Surv Tutor. Security and privacy challenges in connected vehicular cloud computing 22(4):2725–2764
22. Nazih O, Benamar N, Addaim A (2020) An incentive mechanism for computing resource allocation in vehicular fog computing environment. In: 2020 International conference on innovation and intelligence for informatics, computing and technologies (3ICT). IEEE, pp 1–5
23. Nkenyereye L, Islam SR, Bilal M, Abdullah-Al-Wadud M, Alamri A, Nayyar A (2021) Future Gener Comput Syst. Secure crowd-sensing protocol for fog-based vehicular cloud 120:61–75
24. Oham C, Michelin RA, Jurdak R, Kanhere SS, Jha S (2021) B-FERL: blockchain based framework for securing smart vehicles. Inf Process Manage 58(1):102,426
25. Pu Y, Xiang T, Hu C, Alrawais A, Yan H (2020) Inf Sci. An efficient blockchain-based privacy preserving scheme for vehicular social networks 540:308–324
26. Rawat DB, Doku R, Adebayo A, Bajracharya C, Kamhoua C (2020) IEEE Netw. Blockchain enabled named data networking for secure vehicle-to-everything communications 34(5):185–189
27. Subramanian G, Thampy AS (2021) Implementation of hybrid blockchain in a pre-owned electric vehicle supply chain. IEEE Access
28. Sun S, Gu X, Wang J (2020) Research on incentive method of resource sharing in VANET based on game theory. J Phys: Conf Ser 1624:032022 (IOP Publishing)
29. Zeng F, Chen Y, Yao L, Wu J (2021) Peer-to-Peer Netw Appl. A novel reputation incentive mechanism and game theory analysis for service caching in software-defined vehicle edge computing 14(2):467–481
30. Zhang A, Lin X (2018) J Med Syst. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain 42(8):1–18

Unconditionally Fast Secure Multi-party Computation with Multi-depths Gates Using Pre-computed Information

Amirreza Hamidi and Hossein Ghodosi

Abstract In secure multi-party computation (MPC), n participants execute secure communication in a circuit to compute any given function using their private inputs such that the system does not reveal any information about their inputs. Computing a share of n-inputs ($n > 2$) multiplication gates with various multiplicative depths has been an important subject in this research field as it increases the round complexity using, for example, Beaver's triples method. That is because just the shares of the multiplication gates with the same depth can be computed each time of implementing the existing MPC protocols, and thus, the communication rounds of a circuit with different multiplicative levels increase. In this paper, we present a secure protocol which enables computing a share of simultaneous n-inputs multiplication gates as well as the addition gate in just one round of online computation phase. Therefore, our protocol enables computing a share of any given function in just one round of computation which would result in fast computation and gives an improvement on the current MPC systems. To achieve it, we employ the technique of (Theory of cryptography conference. Springer, pp 213-230, [2]), based on hyper-invertible matrices, for generating pre-computed shares of random values. Our protocol has the unconditionally security against a coalition of t parties controlled by a passive adversary with the communication complexity $O(n^2)$ for computing a share of n-inputs multiplication with different depths.

Keywords Fast multi-party computation · Pre-computed Information · Multiplication gates with different depths · Information-theoretic security

A. Hamidi (✉) · H. Ghodosi
James Cook University, Townsville, QLD, Australia
e-mail: amirreza.hamidi@my.jcu.edu.au

H. Ghodosi
e-mail: hossein.ghodosi@jcu.edu.au

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_28

1 Introduction

Secure multi-party computation (MPC) is an important tool which first was introduced by Yao [18] for the boolean circuit and, later [14], extended it to the case with n parties . In the version with information-theoretic security, the system requires t out of n participant to contribute and compute the function using their correct inputs which are called the threshold MPC.

Definition 1 Threshold MPC system enables a set of (t, n) (called t out of n) participants $P_1, \ldots, P_n$, with their inputs $x_1, \ldots, x_n$, to compute any given function $f(x_1, \ldots, x_n)$ without revealing their private inputs.

Any MPC system includes two major types of adversaries which are passive (semi-honest) and malicious (active). A coalition of the parties, who are controlled by a passive adversary, follow the protocol while trying to learn any information including the inputs of honest participants and the correct actual outcome. On the other hand, a malicious adversary deviates from the protocol in an arbitrary fashion using the shares it gives to the protocol [12]. It should be noted that considering a passive adversary is more practical and many MPC systems assume this setting. That is because it is easier to record the contents of some communication activities while following the protocol than changing the outcome of the protocol [11]. Moreover, a player is more likely to compute the correct output of a function while being curious to gain much information about the other parties' inputs. Generally, the computational assumptions of any MPC protocols are based on the level of power limitation assumed for the adversary of the system which can be categorized to computationally bounded or unbounded. The computational power of an adversary is assumed bounded in a computational (cryptographic) secure protocol while it is assumed to be unbounded for in a information-theoretic secure protocol [12]. Thus, the security of the information-theory assumption seems to be stronger as it is not dependent on the computational security assumptions (i.e. it is secure against the adversary with unlimited power computation and time) [15]. Moreover, a MPC protocol is secure if the security conditions are satisfied, which are *Correctness* and *Privacy*. The *Correctness* condition ensures computation of the correct outcome (against an active adversary) while the *Privacy* condition guarantees no information leakage of the honest participants (against a passive adversary). Hence, in the case it is assumed that the players follow the protocol, the correctness condition of the protocol is preserved; however, the protocol must hold a threshold privacy condition. In fact, a MPC protocol is *t-private* in the presence of the total n participants, if the protocol remains private against a maximum number (t) players corrupted by a passive adversary [10].

Definition 2 A t-private MPC protocol reveals no information of the honest participants to any set of up to t passive adversaries in the system.

1.1 Background

After introducing the secure MPC by Yao [18], some early studies were conducted using the cryptographic intractability assumptions [14] and the information-theoretic security [3, 15]. The case of calculating a share of any addition gate(two or more inputs addition) can be implemented using homomorphic property of Shamir's secret sharing [4]. This implies that any linear function (e.g. multiplication by a constant number) can be computed with no interaction. However, a challenging issue arises when two or more participants aim to multiply their inputs using secret sharings of degree t as it impacts the security condition of the system. In detail, assume that P_i and P_j $(1 \leq i, j \leq n, i \neq j)$, holding the inputs x_i and x_j, secret-share the inputs among n parties using the polynomials of degree t $(n \leq 2t)$. If a participant P_k wants to compute a share of $f(x_i, x_j) \leftarrow x_i \times x_j$, he calculates the new share $[x_i x_j]_{2t} \leftarrow [x_i]_t \times [x_j]_t$ where $[x_i]_t$ and $[x_j]_t$ are his corresponding shares of the inputs x_i and x_j. This would cause two major problems; first, the system requires a number of at least $2t + 1$ participants for reconstructing the output that is more than the number of the security threshold. Furthermore, the resulted polynomial is not random contradicting the definition of the information-theoretic security [3].

This problem has attracted some studies such as degree reduction [3, 6]. A study of information-theoretic and perfect security in MPC was conducted by [3] to propose an efficient system, using private channels, with $n \geq 3t + 1$ participants. [9] and, later, [13] presented another technique of redistributing new shares resulting in the same old secret which can belong to the polynomials with lower degree. Beaver suggested a new scheme with an offline pre-processing phase that is secure against passive adversaries by introducing triples as random pre-shared values [1]. In every multiplication gate, one pre-computed triple $(ab = c)$ is generated and t-shared among the participants in an offline phase which each participant utilize to compute a share of the multiplication gate at the cost of two secret reconstructions. Since the introducing of this method, many other studies have employed the idea of distributing computation overhead into different phases. These protocols usually include two different phases:

- **Pre-Processing Phase**: The parties are given some random pre-computed information (e.g. pre-shared triples) in this phase which is used in the online computation phase. This random information can be generated and shared by a trusted third party (in the form of commodity-based cryptography) or by the participants themselves. This technique results in a probabilistic functionality in this phase which preserves the privacy of the inputs in the online computation phase.
- **Computation Phase**: This is where the parties execute the actual computation online using the pre-computed information they hold resulting higher efficiency and cheaper computation cost. Here, the important challenge is that the inputs must remain private despite utilizing the pre-shared information in the protocol.

Many studies have employed the Beaver's circuit randomization technique to present secure MPC protocols in arithmetic circuits [2, 5, 8, 13]. Moreover, some studies proposed that the pre-shared random values can be generated and distributed by a trusted third party (initializer) [7], by cloud service providers [17] or by the players themselves [2, 13]. However, it is more practical and secure not to employ a third party, due to the matter of privacy where it can later collude with the participants and learn their inputs. [2] proposed an efficient secure technique using *hyper-invertible* matrices that enables the players to generate the pre-shared triples.

However, an important limitation of the idea of Beaver's pre-shared triples is that the multiplication gates must not be dependent on each other. In other words, each participant can only compute the shares of the multiplication gates with the same multiplicative depth in the circuit in each communication round. Thus, the shares of the gates with intermediate multiplicative depths, e.g. $f(x_i, x_j, x_k) \leftarrow x_i \times x_j \times x_k$, cannot be computed simultaneously in just one round of communication which increases the round complexity.

1.2 Our Contribution

We aim to propose a fast unconditionally secure MPC protocol to compute a share of any given function $f(x_1, \ldots, x_n)$, including up to simultaneous n-inputs multiplication with intermediate multiplicative depths, in just one round of online computation. We stress the feature of fast computation as the low round complexity of our protocol allows the participants to compute a share of all the multiplication and addition gates in parallel in just one communication round which is an improvement on the current MPC systems using Beaver's triples. Our protocol is operated online in arithmetic circuit and it includes two phases, a setup phase and a computation phase. We employ the technique of hyper-invertible matrices of [2] in a loop to generate random pre-shared values in the setup phase. This technique ensures the privacy of the pre-shared values and, thus, the probabilistic functionality of the setup phase. The protocol is t-private, and the communication complexity to perform n-inputs multiplication gates with different depths is $O(n^2)$.

2 Preliminaries

2.1 Model

We aim to propose a secure MPC protocol that enables $t + 1$ out of n parties (where $n \geq t + 1$) to calculate a share of any given circuit $f(x_1, \ldots, x_n)$ in just one round of computation. Specifically, it is capable of computing a share of simultaneous n-inputs multiplication gates with intermediate multiplicative depths, which belong to the function $f(x_1, \ldots, x_n) \leftarrow \prod_{i=1}^{i=n} x_i$, in one online communication round. Our protocol has two online phases: setup and computation. We employ the hyper-invertible matrices technique of [2] for generating secure double sharings (two Shamir's secret sharing of the same random value with two different thresholds) of random values. In fact, we wish that an input holder generates sharings $[\alpha]_d$ and $[\alpha]_{d'}$ for a random value α, unknown to adversary, where d and d' are two different degrees. This technique enables a pair of input holders P_i and P_j, where $1 \leq i, j \leq n$ $(i \neq j)$, to generate a triple securely in the setup phase [2]. In order to achieve this goal in our model, a number of $n \geq 2t + 1$ players is required to perform the initial computations in the setup phase. Afterwards, using a for-loop for each multiplication gate with the same multiplicative depth would enable each participant to calculate a share of the n-inputs multiplication triple in threshold t. Finally, the random t-sharings, generated in the setup phase, can be utilized to compute any given function consisting of the addition gate and the multiplication gates with various intermediate levels in parallel.

2.2 Shamir's Secret Sharing

This threshold secret sharing scheme, which has important application to any distributed systems, includes n parties and a dealer (secret holder). The goal of the dealer is to distributes his secret s among all the participants using a random polynomial of degree t with the free term s as $(f(x) = s + a_1x + a_2x^2 + \ldots + a_tx^t \quad mod\, q)$ and, assuming the private channels are secure, each party P_i is given the share $f_i \leftarrow f(x_i)$ [16]. The dealer randomly chooses the coefficients a_1, a_2,. . ., a_t, and the field operation is in $\mathbb{F}_q$ where q is a prime number with the condition $q > n$. A set of Shmair shares $(f_1, \ldots, f_n)$ of the secret s computed with the threshold (degree) d is denoted by $[s]_d$ in this paper. This secret sharing scheme is linear, and a share of any linear function of the inputs can be calculated with no interaction by having that the shareholder P_i apply the same linear function to the respective shares he has received [4]. The polynomial $f(x)$ can be interpolated by having any subset of at least $t + 1$ participants pool their shares and reconstruct the correct free term s, whereas any subset of less than $t + 1$ parties can gain no information about the correct secret (i.e. this scheme is a (t, n) threshold secret sharing).

We use t-sharings (denoted by $[.]_t$) of Shamir's scheme in the computation phase, and also double sharings, (denoted as $[.]_t$ and $[.]_{2t}$ with the thresholds t and $2t$) in the setup phase of our protocol.

2.3 Generating t-Sharings of Randomness Based on Hyper-Invertible Matrices

We employ the technique of [2] to compute sharings of n random shared values in the setup phase of our model. The method is based on hyper-invertible matrices to generate double sharings of a random value. Note that due to the limited space, the important concepts and protocols are described here; however, it is recommended to refer to [2] for some other tools and the security proofs.

In order to generate double sharings $[r]_d$ and $[r]'_d$ of a random value r, we need to define the concept of hyper-invertible matrices based on [2], where a way of constructing the matrix M is presented.

Definition 3 A hyper-invertible matrix has the size $m \times n$ where for any sets of rows $R \subseteq \{1, \ldots, m\}$ and columns $C \subseteq \{1, \ldots, n\}$ with $|R| = |C| > 0$, the matrix M_R^C is invertible, such that it consists of the intersections between rows in R and columns in C.

It has an important property where any mapping of n points, for example $(x_1, \ldots, x_n)$ to $(y_1, \ldots, y_n)$, can be calculated using two sets of fixed elements. This feature enables a mapping of any n input values using a linear function of the remaining n input values.
Based on the proposed technique on [2] for generating triples, each player P_i distributes a random value s_i, of degrees t and t', to the other participants using Shamir sharing. Each player now holds two vectors of the shares $[s_1]_{t,t'}, \ldots, [s_n]_{t,t'}$ and he can compute two new vectors of shares, using the hyper-invertible matrix M, as follows:

$$([r_1]_{t,t'}, \ldots, [r_n]_{t,t'}) = M([s_1]_{t,t'}, \ldots, [s_n]_{t,t'})$$

Such that each set of the sharings $[r_i]_t$ lies on the polynomial $h(.)$ of degree t, and the value r_i is private against t adversaries. Thus, the double sharings $[r_1]_{t,t'}, \ldots, [r_n]_{t,t'}$ are the output for each player.

In order to generate random triples of degree t in a pre-processing phase, given sharings $[a_i]_t$, $[b_i]_t$ and $[r_i]_{2t}$ of the random values a_i, b_i and r_i, each player computes a share, which belongs to a polynomial of degree $2t$, as follows:

$$[d_i]_{2t} = [a_i]_t[b_i]_t - [r_i]_{2t} = [a_ib_i - r_i]_{2t}$$

and at least $2t + 1$ players pool their shares $[d_i]_{2t}$ and publicly reconstruct the value d_i. Finally, each player locally computes his new share $[c_i]_t$ as follows:

$$[c_i]_t = d_i + [r_i]_t = a_ib_i - r_i + [r_i]_t$$

Now, each player holds shares of $[c_i]_t \leftarrow [a_ib_i]_t$, $[a_i]_t$ and $[b_i]_t$. Each value of a_ib_i is clearly t-private and the communication complexity for generating one set of the double sharing $[r_i]_{t,2t}$ and the triple $[a_i]_t$, $[b_i]_t$ and $[a_ib_i]_t$ is $O(n)$, and, thus, for n sets is $O(n^2)$ [2].

2.4 Security Conditions

As discussed in Sect. 1, The security requirements of any MPC protocol with n participants must be satisfied. let the parties with holding the inputs $x_1, \ldots, x_n$, want to compute any function $f(x_1, \ldots, x_n)$. The protocol must meet the following requirements:

- **Correctness**: Each party P_k gets the correct output of the polynomial $f(x_1, \ldots, x_n)$ after executing the protocol.
- **Privacy**: The inputs of the honest participants are private against a coalition of t parties corrupted by a passive adversary (i.e. the passive adversary cannot obtain any information about the inputs of honest participants, except what he can gain from the actual outcome after executing the protocol).

3 Our Protocol

Our protocol is designed to have just one setup phase for both addition gate and multiplication gates, and one computation phase for calculating a share of any given polynomial. Note that the computation of all the multiplication gates with different multiplicative levels can be conducted in parallel as well. Moreover, a share of any n-inputs addition gate can be computed in one round of the protocol. The private communication lines between each pair of players are assumed to be secure.

1. **Setup phase**: In this phase, each input holder generates a random value and shares it among the players. Depending on the existing multiplicative depths, the players use the hyper-invertible matrices and a loop to compute t-shaings of multiplying the random values.
2. **Computation phase**: In this phase, each participant computes a share of the given function including n-inputs addition and n-inputs multiplication with different depths. The shares of the both gates can be computed in parallel. Thus, a share of any given function can be computed in just one round of online computation phase.

3.1 Setup Phase

Let assume that a given function $f(x_1, \ldots, x_n)$ has the gates of n-inputs multiplication with $n - 1$ different multiplicative depths. Using the result discussed in Sect. 2.3 and in [2], Fig. 1 shows the detail of the setup phase.

The probabilistic functionality of this phase ensures the privacy of inputs in the computation phase. It should be stated that this phase can be implemented in parallel

- Each input holder P_i (for $i = 1, \ldots, n$) generates a random number γ_i (where $\gamma_i \neq 0$) and distributes it, using sharings $[\gamma_i]_t$, among the participants.
- Also, each input holder generates a random value s_i and shares it in double sharings $[s_i]_{t,2t}$ among the participants.
- Each player P_k locally computes two vectors of double sharings $[r_i]_{t,2t}$ using hyper-invertible matrices described in section 2.3 as:

$$([r_1]_{t,2t'}, \ldots, [r_n]_{t,2t}) = M([s_1]_{t,2t'}, \ldots, [s_n]_{t,2t})$$

- In the gates of multiplying n inputs $f(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i$, for each pair of the inputs multiplication $x_i x_j$ with the same depth, where $j \leftarrow i + 1$, while $j \leq n$ (executing a loop):
  - Each player P_k computes a $2t$-sharing as follows:

$$[\gamma_i]_t[\gamma_j]_t - [r_i]_{2t} = [\gamma_i\gamma_j - r_i]_{2t}$$

  - A set of $2t + 1$ participants reconstructs the value $\gamma_i\gamma_j - r_i$.
  - Each player P_k computes the new t-sharing as:

$$[\gamma_i\gamma_j]_t = \gamma_i\gamma_j - r_i + [r_i]_t$$

  - The players execute $i \leftarrow i + 1$ and $[\gamma_i]_t \leftarrow [\gamma_i\gamma_j]_t$. Note that the new local sharings $[\gamma_i]_t$ inside the loop is different from the initial sharings each input holder distributes as the local sharings change depending on the multiplicative depths of the gates.
  - if $i = n$, P_k returns the t-sharing $[\gamma_1 \times \ldots \times \gamma_n]_t \leftarrow [\gamma_i]_t$.

Output: Each player P_k holds the set of t-sharings $([\gamma_1]_t, \ldots, [\gamma_n]_t)$ and $[\gamma_1 \times \ldots \times \gamma_n]_t$.

Fig. 1 Setup phase of our proposed protocol

for all n-inputs multiplication gates $\prod_{i=1}^{m} x_i$ $(m \leq n)$ in the function $f(x_1, \ldots, x_n)$. The communication upper bound for computing a share of a multiplication gate in this phase is $O(n)$ thus, for a n-inputs multiplication it equals $O(n^2)$.

3.2 Computation Phase

In this phase, each participant P_k can compute a share of the given function in just one round of communication (i.e. the computation of both n-inputs addition and multiplication gates can be performed in parallel). All the participants commence this phase while they are holding the sharings $[\gamma_i]_t$ $(i = 1, \ldots, n)$ and $[\prod_{i=1}^{n} \gamma_i]_t$. Figure 2 illustrates the computation phase of our protocol.

Note that the amounts of inputs cannot be zero using the proposed protocol. However, it doesn't affect the correctness since, in any MPC circuit, if a mathematical term in a function $f(x_1, \ldots, x_n)$ has a zero input, we can remove that term and it doesn't affect the outcome as well as the privacy of the other inputs. The fact that this protocol can compute a share of any given function (including any addition and multiplication gates with intermediate multiplicative depths) in just one communication round, would result in a fast computation phase. That is, a share of any given function can be computed in just one online round of computation phase using the protocol, which gives an improvement on the round complexity of the current MPC systems. The computation phase has the communication upper bound of $O(n^2)$ as well.

Input: The players $P_1, \ldots, P_n$ hold the inputs $x_1, \ldots, x_n$.
Output: Each player P_k, among a set of $t+1$ or more participants $(1 < t+1 \leq n)$, computes a share of the given function $f(x_1, \ldots x_n)$.

- Each input holder calculates a random value α_i as:

$$\alpha_i = \frac{\gamma_i}{x_i}$$

  And he distributes it using the sharings $[\alpha_i]_t$ among the participants.
- A set of $t+1$ participants reconstructs the values α_i (for $i = 1, \ldots, n$).

Addition

- Each participant P_k computes the new share of up to n-inputs addition as follows:

$$[x_1 + \ldots + x_n]_t = \sum_{i=1}^{n} \frac{[\gamma_i]_t}{\alpha_i}$$

Multiplication

- Each participant P_k can compute the new share of n-inputs multiplication gates as follows:

$$[x_1 \times \ldots \times x_n]_t = \frac{[\prod_{i=1}^{n} \gamma_i]_t}{\prod_{i=1}^{n} \alpha_i}$$

Fig. 2 The computation phase of our proposed protocol

3.3 Security Analysis

We assess the protocol with regards to the security requirements. Please refer to Sect. 2.3 and [2] for security assessment of the random sharings $[\prod_{i=1}^{n} \gamma_i]_t$ generated in the setup phase.

Correctness

Theorem 1 *After executing the protocol, each party* P_k $(1 \leq k \leq t+1)$ *computes the correct share of the polynomial* $f(x_1, \ldots, x_n)$.

Proof After the setup phase, each participant holds the sharings $[\gamma_i]_t$ and $[\prod_{i=1}^{n} \gamma_i]_t$. In the beginning of the current phase, the players reconstruct the random values α_i $(\alpha_i \neq 0)$. For the n-inputs addition gate, each player P_k holds the following share:

$$f_k = \frac{[\gamma_1]_t}{\alpha_1} + \ldots + \frac{[\gamma_n]_t}{\alpha_n}$$

where, according to the linear feature of Shamir's secret sharing scheme, f_k belongs to a polynomial with the the free term:

$$\begin{aligned} f(x_1, \ldots, x_n) &= \frac{\alpha_1 x_1}{\alpha_1} + \ldots + \frac{\alpha_n x_n}{\alpha_n} \\ &= x_1 + \ldots + x_n \end{aligned}$$

Similarly, for the n-inputs multiplication with different multiplicative depths, each P_k holds the following share:

$$f_k = \frac{[\gamma_1 \times \ldots \gamma_n]_t}{\alpha_1 \times \ldots \times \alpha_n}$$

Where f_k belongs to a polynomial with the constant term:

$$\begin{aligned} f(x_1, \ldots, x_n) &= \frac{(\alpha_1 x_1) \times \ldots \times (\alpha_n x_n)}{\alpha_1 \times \ldots \times \alpha_n} \\ &= x_1 \times \ldots \times x_n \end{aligned}$$

Privacy

Theorem 2 *The proposed protocol preserves the privacy against a coalition of t players corrupted by a passive adversary.*

Proof The probabilistic functionality of hyper-invertible matrices technique, described in Sect. 2.3, ensures the privacy of the double sharings $[r_i]_{t,2t}$ and, thus, the random values $\gamma_i \leftarrow x_i \alpha_i$. Moreover, the for loop utilized to generate the sharings $[\gamma_i \gamma_j]_t$ preserves the privacy against a coalition of t players corrupted by a passive adversary. Hence, the setup phase outputs the sharings $[\gamma_1 \times \ldots \times \gamma_n]_t$ which are t-private.

Without loss of generality, let assume that a coalition of t players, (not including P_1) corrupted by a passive adversary, has the view denoted by $\text{VIEW}_{\mathcal{A}}$. Note that, as we mention in the protocol, the inputs cannot be zero ($x_i \neq 0$). For the gate of n-inputs addition in the computation phase $\text{VIEW}_{\mathcal{A}}$ is:

$$f_2 = \frac{[\gamma_1]_t}{\alpha_1} + \cdots + \frac{[\gamma_n]_t}{\alpha_n}$$

$$f_3 = \frac{[\gamma_1]_t}{\alpha_1} + \cdots + \frac{[\gamma_n]_t}{\alpha_n}$$

$$\vdots$$

$$f_{t+1} = \frac{[\gamma_1]_t}{\alpha_1} + \cdots + \frac{[\gamma_n]_t}{\alpha_n}$$

where, according to the threshold secret sharing, the term $\frac{[\gamma_1]_t}{\alpha_1}$ is private against $\text{VIEW}_{\mathcal{A}}$.

Furthermore, $\text{VIEW}_{\mathcal{A}}$ for n-inputs multiplication gates is:

$$f_2 = \frac{[\gamma_1 \times \cdots \times \gamma_n]_t}{\alpha_1 \times \cdots \times \alpha_n}$$

$$f_3 = \frac{[\gamma_1 \times \cdots \times \gamma_n]_t}{\alpha_1 \times \cdots \times \alpha_n}$$

$$\vdots$$

$$f_{t+1} = \frac{[\gamma_1 \times \cdots \times \gamma_n]_t}{\alpha_1 \times \cdots \times \alpha_n}$$

where $\text{VIEW}_{\mathcal{A}}$ can gain no information about the free term of the sharings $[\gamma_1 \times \ldots \times \gamma_n]_t$ generated in the setup phase. Hence, the proposed protocol is t-private.

4 Conclusion

In this paper, we propose a protocol with information-theoretic security to compute any given function including simultaneous n-inputs multiplication gates, with different multiplicative depths, in a MPC circuit. Indeed, our protocol can be used to calculate a correct share of n-inputs addition gate and n-inputs multiplication gates in parallel in just one online round of computation. This would result in a fast computation technique, as a share of any given function can be computed in one online computation round which gives an improvement on the round complexity of current MPC protocols. In other words, it improves the round communication of the protocols using Beaver's triples method since they must be implemented in $n - 1$ separate rounds for computing the n-inputs multiplication gates in a circuit. Our protocol is online and has two phases: setup phase and computation phase. We employ the hyper-invertible matrices technique of [2] in the setup phase to generate private pre-computed t-sharings which are utilized in the actual computation phase. Our protocol is t-private, and the communication complexity for computing the n-inputs multiplication gates is $O(n^2)$.

References

1. Beaver D (1991) Efficient multiparty protocols using circuit randomization. In: Annual international cryptology conference. Springer, pp 420–432
2. Beerliová-Trubíniová Z, Hirt M (2008) Perfectly-secure MPC with linear communication complexity. In: Theory of cryptography conference. Springer, pp 213–230
3. Ben-Or M, Goldwasser S, Wigderson A (2019) Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Providing sound foundations for cryptography: on the work of Shafi Goldwasser and Silvio Micali, pp 351–371

4. Benaloh JC (1986) Secret sharing homomorphisms: Keeping shares of a secret secret. In: Conference on the theory and application of cryptographic techniques. Springer, pp 251–260
5. Bendlin R, Damgård I, Orlandi C, Zakarias S (2011) Semi-homomorphic encryption and multiparty computation. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, pp 169–188
6. Chaum D, Crépeau C, Damgard I (1988) Multiparty unconditionally secure protocols. In: Proceedings of the twentieth annual ACM symposium on theory of computing, pp 11–19
7. Cianciullo L, Ghodosi H (2018) Efficient information theoretic multi-party computation from oblivious linear evaluation. In: IFIP international conference on information security theory and practice. Springer, pp 78–90
8. Damgård I, Pastro V, Smart N, Zakarias S (2012) Multiparty computation from somewhat homomorphic encryption. In: Annual cryptology conference. Springer, pp 643–662
9. Gennaro R, Rabin MO, Rabin T (1998) Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In: Proceedings of the seventeenth annual ACM symposium on Principles of distributed computing, pp 101–111
10. Ghodosi H, Pieprzyk J (2009) Multi-party computation with omnipresent adversary. In: International workshop on public key cryptography. Springer, pp 180–195
11. Goldreich O (1998) Secure multi-party computation. Manuscript. Preliminary version 78
12. Goldwasser S (1997) Multi party computations: past and present. In: Proceedings of the sixteenth annual ACM symposium on Principles of distributed computing, pp 1–6
13. Hirt M, Maurer U, Przydatek B (2000) Efficient secure multi-party computation. In: International conference on the theory and application of cryptology and information security. Springer, pp 143–161
14. Micali S, Goldreich O, Wigderson A (1987) How to play any mental game. In: Proceedings of the nineteenth ACM symposium on theory of computing, STOC. ACM, pp 218–229
15. Rabin T, Ben-Or M (1989) Verifiable secret sharing and multiparty protocols with honest majority. In: Proceedings of the twenty-first annual ACM symposium on theory of computing, pp 73–85
16. Shamir A (1979) Commun ACM. How to share a secret 22(11):612–613
17. Smart NP, Tanguy T (2019) Taas: Commodity MPC via triples-as-a-service. In: Proceedings of the 2019 ACM SIGSAC conference on cloud computing security workshop, pp 105–116
18. Yao AC (1982) Protocols for secure computations. In: 23rd annual symposium on foundations of computer science (SFCS 1982). IEEE, pp 160–164

Real-Time Pain Detection Using Deep Convolutional Neural Network for Facial Expression and Motion

Kornprom Pikulkaew, Waraporn Boonchieng, and Ekkarat Boonchieng

Abstract At present, in every corner of the world, including developing and developed, countries got affected by infectious diseases such as the COVID-19 virus. Our objective was to create a real-time pain detection for everyone that can use it by themselves before going to the hospital. In this research, we used a dataset from the University of Northern British Columbia (UNBC) and the Japanese Female Facial Expression (JAFFE) as a training set. Furthermore, we used unseen data from webcam or video as a testing set. In our system, pain is divided into three categories: mild, moderate-to-severe-to-painful, and severe. The system's efficiency was assessed by contrasting its results with those of a highly qualified physician. Classification accuracy rates were 96.71, 92.16, and 98.40% for the not hurting, getting uncomfortable, and painful categories. To summarize, our research has created a simple, cost-effective, and readily understood alternate method for the general public and healthcare professionals to screen for pain before admission.

Keywords Deep convolutional neural network · Facial expression · Motion vector · Pain detection · Real-time system

K. Pikulkaew (✉) · E. Boonchieng
Department of Computer Science and Graduate School, Faculty of Science, Chiang Mai University, Chiang Mai, Thailand
e-mail: champ_mekung@hotmail.com

E. Boonchieng
e-mail: ekkarat@boonchieng.net

W. Boonchieng
Faculty of Public Health, Chiang Mai University, Chiang Mai, Thailand
e-mail: woraporn.b@cmu.ac.th

E. Boonchieng
Department of Computer Science and Data Science Research Center, Faculty of Science, Chiang Mai University, Chiang Mai, Thailand

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_29

1 Introduction

Nowadays, we cannot deny that pain occurs daily and affects people of all sexes and ages. In particular, the world's present predicament with the COVID-19 virus demonstrates how beneficial it would be to have a technique that analyzes the disease's first discomfort before referring patients to the hospital in severe instances. When it becomes essential to go to the hospital, extra costs will occur. Comprehensive treatment is not feasible given the hospital's present condition, which indicates a high patient load. In addition to the stress and strain that physicians and nurses face, as a result, if a pain detecting system is utilized to address this issue, it may be an ideal solution. The facial action units (AUs) system, which developed from the facial action coding system (FACS), may be used to recognize faces for pain detection [1].

The pain unit is derived from FACS, a technology that detects facial muscle activity. The FACS method [2] was historically used to evaluate sadness and quantify pain in individuals who could not speak [3]. The FACS prototype was created for non-human primates such as chimps, dogs, and horses. Later modifications to the emotional facial action coding system (EMFACS) allowed the detection of anger, sorrow, and regret [4]. Finally, a consistent method for human pain detection was developed. Numerous researchers [5–7] collected data from the UNBC dataset of patients with shoulder discomfort, and images illustrate patients' straight faces. Active means that patients can move their shoulders independently, while passive means that medical personnel can assist patients in moving their shoulders. UNBC contains 50,000 images of patients, both males and women. However, UNBC images did not show an imbalance in the intensity of pain for either kind. Some are excessively numerous, while others are excessively few. Therefore, data optimization techniques such as imbalance methodology [8], generative adversarial network (GAN) [9], and augmented data approaches are required to minimize imbalance.

This technique detects moving faces and postures using a sequential picture of human faces from the UNBC and JAFFE datasets [10, 11]. Our approach is built on unsupervised learning, in contrast to other researchers who emphasize supervised learning. We chose semi-supervised learning since, in the actual world, we cannot classify all pictures to train a machine learning system, and the systems must learn on their own. As a result, this will challenge the computer, as the testing set will include data that the system has never seen before.

This research suggests using deep convolutional neural network (DCNN) methods to detect and categorize facial discomfort in real-time. The findings are compared to ground truth obtained by medical personnel.

2 Methodology

2.1 Data Collection

We used the UNBC [10] and JAFFE [11] datasets to create this facial expression sequence. About 50,000 images are stored in 225 files across 25 different themes at the UNBC. There was a total of 63 men and 66 women within the group that had shoulder pain. When it comes to facial expressions, JAFFE only offers 213 images with seven different staged poses. These include six different basic poses and one neutral pose. A significant difference between the JAFFE dataset and others is that it collected an 8-bit grayscale image of each subject.

There are 44 action units (AUs) assigned to each human facial activity depending on personal characteristics. This operation was carried out in the first phase by Prkachin and Solomon [12] with the help of AU4-AU43. It was discovered that just AU4, AU6 were needed since they included so much information about pain; each activity was divided into five intensity levels (1 = minimum, 5 = maximum).

2.2 Scale for Assessing Pain Based on Action Units

Our real-time pain detection system made use of AUs to quantify pain. The reason AUs are reliable and accurate is because they have been validated in the medical field by MDs [13]. We calculated pain using the Prkachin and Solomon pain intensity (PSPI) equation [12]. The pain is defined in Eq. 1. In addition, as shown in Fig. 1, our approach separates pain into three categories: not painful, getting uncomfortable, and severe.

$$\text{Pain} = \text{AU4} + \max(\text{AU6}||\text{AU7}) + \max(\text{AU9}||\text{AU10}) + \text{AU43}, \tag{1}$$

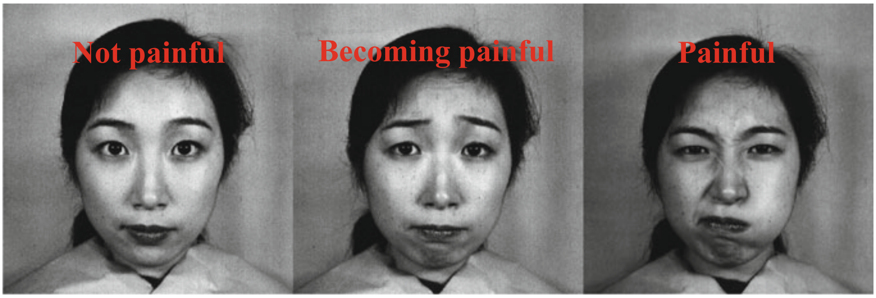


Fig. 1 An example of a pain category based on the PSPI

2.3 Deep Convolutional Neural Network and Facial Identification Process

OpenCV was used to improve facial recognition. For pain analysis, the DCNN works well when used with an AAM to identify AUs in each patient picture. ResNet-34, a method for image recognition developed by He et al. [14] is the foundation of our face recognition architecture. The network was trained using almost three million images from the wild dataset of labeled faces. The marker was then generated using the training data from the UNBC and JAFFE sets. To increase the system's speed and accuracy, labels must be drawn. The movement was used with the coordinates of reference pictures to predict the axis of the decoded image.

Convolutional neural networks (CNNs), a kind of neural network, are used to classify images, cluster them based on similarity, and identify objects within scenes. The most widely used computer method for image recognition is convolutional neural networks (CNNs). The number 34 refers to the number of layers in the CNN used in our pain detecting algorithm. A DCNN is a stack of neural networks that has been combined into a single model. In other words, DCNN is just an enhanced version of CNN.

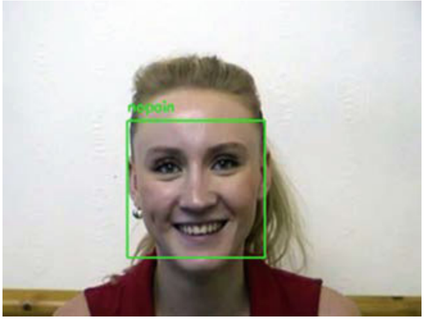
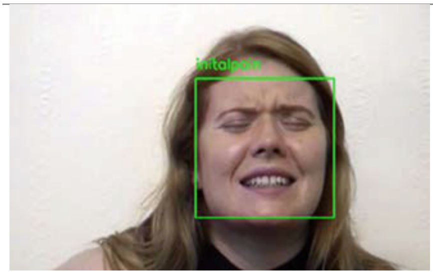
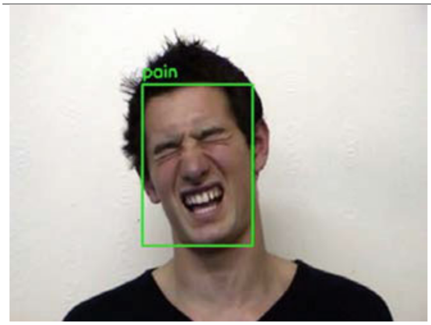
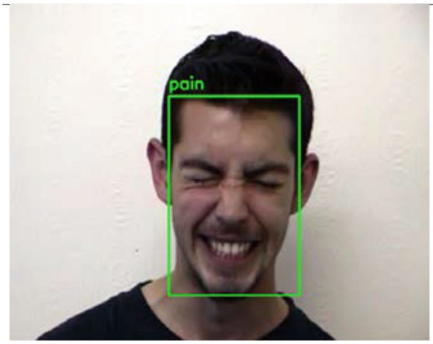
2.4 Real-Time System

Python, OpenCV, and deep learning were used to build our real-time system. We utilized two more libraries to improve accuracy and speed:

1. Davis King's dlib library [15]
2. Adam Geitgey's facial recognition [16].

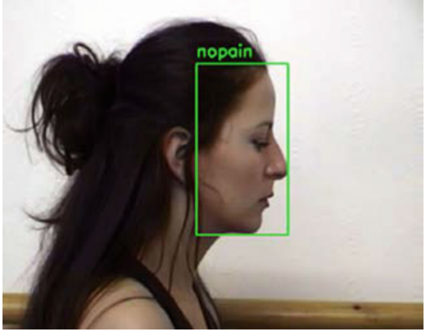
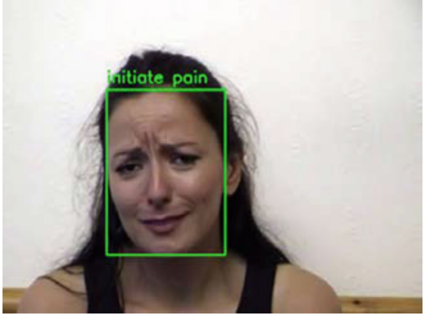
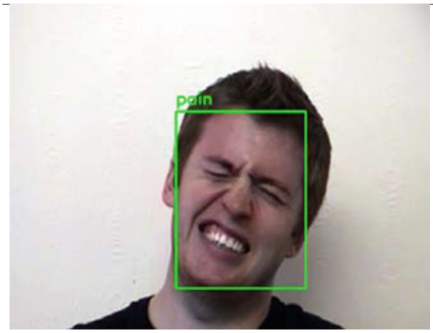
Pain may be detected using static pictures, video feeds, or a webcam. This study aims to develop a real-time system that anybody, particularly medical personnel, can use. However, running on a CPU has certain drawbacks since it consumes many resources and affects frames per second (FPS). We utilized the GPU to execute the DCNN pain detector to address this issue. Alternatively, the histogram of oriented gradient (HOG) technique must be used to utilize a CPU. The primary difference between DCNN and HOG is in terms of speed and accuracy. The CNN technique is more precise but slower, while the HOG method is quicker but less precise.

Table 1 An illustration of real-time pain detection in human faces

Model	Pain level	Accuracy (%)
	Not painful	96.71
	Becoming painful	90.02
	Painful	85.74
	Painful	98.40

(continued)

Table 1 (continued)

Model	Pain level	Accuracy (%)
	Not painful	84.08
	Becoming painful	92.16
	Painful	97.47

3 Result and Discussion

3.1 Deep Learning-Based Real-Time Pain Detection

The technique for detecting pain in real-time is illustrated in Table 1. The results indicated that the system performed admirably despite the semi-supervised nature of the test data, and the system has never encountered a patient's face. Given that the training dataset consists only entirely of sequential images from the UNBC and

JAFFE databases, it can be argued that the system is capable of being employed in complex situations, whether they involve real-time photos from webcams or video of a patient's discomfort. However, our system is not without flaws. For instance, when DCNN is used, it requires a large amount of data to process. Otherwise, accuracy will decrease. Another factor is GPU-based, as we need to support patients in their daily lives and thus prioritize accuracy over speed.

Although the accuracy may be less than obtained by supervised learning, as an example in the author's previous work [17–19], the objective of this study is to develop a real-time detection system that applies to virtually every situation. As a result, it is the most receptive technique.

3.2 Procedures for Validation and Assessment

Empirical evidence is frequently the only way to tell whether a model works as expected in terms of belief and validity. A model's accuracy, f1-score, and recall are all essential considerations in the evaluation process. As well as utilizing classification criteria, we validated our model with various batch sizes and epochs (time intervals). The test findings are shown in Table 2, which summarizes the data.

Thus, we can summarize the variables used for validation as follows. Accuracy is calculated as the proportion of accurate classifications. The precision is the proportion of relevant outcomes, whereas recall is the proportion of relevant results adequately categorized by the model.

Table 2 The output of our algorithm for detecting pain

Epoch	Batch size	Recall	F1-score	Precision (%)
10	32	0.98	0.98	98
	64	0.99	0.99	99
	128	0.99	0.99	99
15	32	0.98	0.98	98
	64	0.98	0.98	98
	128	0.99	0.99	99
50	32	0.98	0.98	98
	64	0.99	0.99	99
	128	0.99	0.99	99

4 Conclusions

According to the research presented in this article, deep learning can be used to identify pain in real-time in patients' daily lives and hospitals. The method was validated in individuals who complained of pain or discomfort. Standard techniques cannot manage the situations that our approach addresses. Additionally, we suggested a method for increasing the efficiency and accuracy of pain perception by monitoring circumstances and other complicated settings using deep convolutional neural networks.

Our research projects will include accompanying pictures to account for varying pain intensity across the first and second pain classes. Thus, methods such as GAN, the imbalance method, and data augmentation will be utilized to enhance process precision. According to the study presented in this article, deep learning approaches such as 2D facial expression and movement beat more conventional methods in terms of accuracy and cost. Depending on the results, this technique may find use elsewhere in medical research. For instance, facial recognition can identify criminals, and pain may be used to diagnose contagious diseases.

As part of our future research, we intend to replace motion vectors with the optical flow because the result of this study does not provide the best motion estimation to support all degrees of freedom (DF) when the patient moves the body. Additionally, the limitations of our work are dependent on the GPU to achieve the highest accuracy. We intend to enhance our system in the future to support CPUs.

Acknowledgements This research was supported by Chiang Mai University in Thailand, Professor Jee-In Kim, and the Social Echo-Tech Institute at Konkuk University in Seoul, Korea. We are also thankful to the Thailand Research Fund for funding our research under the Royal Golden Jubilee Ph.D. scheme (Grant No. PHD/0226/2561). Furthermore, this work researched either human subjects or animals. The Local Ethics Committee at Chiang Mai University's Faculty of Public Health approved all ethical and experimental procedures and protocols under approval certification no. ET028/2021.

References

1. Hicks CL, Von Baeyer CL et al (2001) The faces pain scale-revised: toward a common metric in pediatric pain measurement. Pain 93:173–183
2. Doody O, Bailey ME (2017) Understanding pain physiology and its application to person with intellectual disability. J Intellect Disabil 23:5–18
3. LNCS Homepage. https://link.springer.com/chapter/10.1007/978-3-319-04627-3_2. Accessed 17 Oct 2021
4. Vijayanandh R, Balakrishnan G (2010) Human face detection using color spaces and region property measures. In: IEEE international conference on robotics and vision
5. Haque MA, Moeslund TB (2018) Deep multimodal pain recognition: a database and comparison of spatio-temporal visual modalities. In: Automatic face & gesture recognition
6. Bargshady G, Zhou X, Wang H (2020) Enhanced deep learning algorithm development to detect pain intensity from facial expression images. Expert Syst Appl 149:1–10

7. Hammal Z, Cohn JF (2012) Automatic detection of pain intensity. In: Multimodal interaction
8. Mikolajczyk A, Grochowski M (2018) Data augmentation for improving deep learning in image classification problem. In: Conference on interdisciplinary Ph.D. workshop
9. Goodfellow I, Pouget-Abadie J et al (2014) Generative Adversarial Nets. Red Hook
10. Lucey P, Cohn JF et al (2012) Painful data: the UNBC-McMaster shoulder pain expression archive database. Image Vis. Comput. J. 30:197–205
11. Michael L, Shigeru A et al (1998) Coding facial expressions with Gabor wavelets. In: IEEE international conference on automatic face and gesture recognition
12. Prkachin KM, Solomon PE (2008) The structure, reliability and validity of pain expression: evidence from patients with shoulder pain. Pain 139:267–274
13. Lucey P, Cohn JF et al (2012) Painful data: the UNBC-McMaster shoulder pain expression archive database. In: Automatic face & gesture recognition
14. He K, Zhang X et al (2020) Deep residual learning for image recognition. In: Computer vision and pattern recognition
15. Dlib Homepage. http://dlib.net. Accessed 17 Oct 2021
16. Adam Homepage. https://www.adamgeitgey.com. Accessed 17 Oct 2021
17. Pikulkaew K, Boonchieng E et al (2020) Pain detection using deep learning with evaluation system. In: Congress on information and communication technology
18. Pikulkaew K, Chouvatut V (2021) Enhanced pain detection and movement of motion with data augmentation based on deep learning. In: Conference on knowledge and smart technology
19. Pikulkaew K, Boonchieng W et al (2021) 2D Facial expression and movement of motion for pain identification with deep learning methods. IEEE Access 9:109903–109914

Machine Learning Analysis in the Prediction of Diabetes Mellitus: A Systematic Review of the Literature

Marieta Marres-Salhuana, Victor Garcia-Rios, and Michael Cabanillas-Carbonell

Abstract In recent years, diabetes mellitus has increased its prevalence in the global landscape, and currently, due to COVID-19, people with diabetes mellitus are the most likely to develop a critical picture of this disease. In this study, we performed a systematic review of 55 researches focused on the prediction of diabetes mellitus and its different types, collected from databases such as IEEE Xplore, Scopus, ScienceDirect, IOPscience, EBSCOhost and Wiley. The results obtained show that one of the models based on support vector machine algorithms achieved 100% accuracy in disease prediction. The vast majority of the investigations used the Weka platform as a modeling tool, but it is worth noting that the best-performing models were developed in MATLAB (100%) and RStudio (99%).

Keywords Diabetes mellitus · Machine learning · Predictive · Systematic review

1 Introduction

Over the years, diabetes has become a global public health problem. Recent studies show that more than 381 million people over the age of 18 suffer from diabetes, and that approximately 45.8% of them have not yet been diagnosed [1]. This disease is classified into three types. Type 1 diabetes is caused by insulin deficiency. Type 2 diabetes is caused by varying degrees of insulin resistance, altered insulin secretion, increased glucose production and various genetic metabolism defects in the action of insulin. Finally, gestational diabetes occurs in women during pregnancy [2]. Now, most physicians would agree that this disease, largely related to one's

M. Marres-Salhuana · V. Garcia-Rios
Universidad Autónoma del Perú, Lima, Perú
e-mail: mmarres@autonoma.edu.pe

V. Garcia-Rios
e-mail: vgarciar@autonoma.edu.pe

M. Cabanillas-Carbonell (✉)
Universidad Privada del Norte, Lima, Perú
e-mail: mcabanillas@ieee.org

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_30

lifestyle, can be prevented; unfortunately, the medical community has been largely absent from the battle to improve these conditions. In fact, numerous studies show that physicians often discuss weight management, physical activity or proper nutrition in <40% of the people they see in their offices [3]. In recent years, humanity has been immersed in health problems, especially in low-income environments, and the situation is aggravated by the limited capacity of the health system [4].

2 Methodology

2.1 Type of Study

For the preparation of the article, the systematic review of the scientific literature will be used; this is a process that allows the collection of relevant evidence on a given topic; in addition, it adjusts to the established eligibility criteria, which allow obtaining answers to the research questions formulated [5].

2.2 Research Questions

RQ1. Which diabetes mellitus prediction models have shown the best results according to performance metrics over the past 4 years?

RQ2. Which tools and languages are the most widely used in the world to develop or implement machine learning models for diabetes mellitus prediction?

RQ3. Which countries have the most research related to the prediction of diabetes mellitus been conducted in the last 4 years?

RQ4. What type of diabetes mellitus has had the highest amount of scientific research focused on prediction with machine learning worldwide?

2.3 Search Strategies

Based on the questions posed, an exhaustive search of articles published in the main databases such as IEEE Xplore, Scopus, ScienceDirect, IOPscience, EBSCOhost and Wiley were carried out, from which 683 scientific articles from the last 4 years were collected. The following formulas were used to search for diabetes-related research: “REDICTION OF DIABETES BY MACHINE LEARNING NOT DEEP LEARNING NOT RISK.”

In order to make an optimal selection of research, search formulas and key words were applied, as well as inclusion and exclusion criteria, and finally, discarding due to duplicity, obtaining 55 relevant papers in Fig. 1.

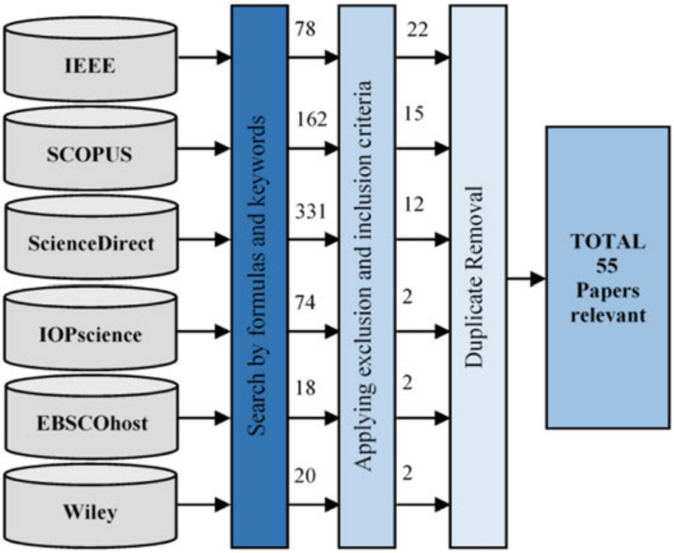


Fig. 1 Selection methodology diagram

2.4 Inclusion and Exclusion Criteria

Inclusion and exclusion criteria presented in the following table were applied for the systematic review study in Table 1:

A total of 683 articles were analyzed, of which 3 duplicate articles were discarded. Then, 55 articles were selected, excluding 628 according to the exclusion criteria

Table 1 Inclusion and exclusion criteria

	Criterion	
Inclusion	I01	Articles related to the development or performance comparison of diabetes mellitus prediction models
	I02	Articles related to the application or implementation of machine learning models for the prediction of diabetes mellitus
	I03	Articles related to the prediction of type 1 diabetes, type 2 diabetes or gestational diabetes using machine learning
Exclusion	E01	Articles unrelated to the development of machine learning models for the prediction of diabetes mellitus
	E02	Articles unrelated to the implementation of machine learning models for diabetes prediction
	E03	Articles unrelated to the prediction of type 1 diabetes, type 2 diabetes or gestational diabetes using machine learning

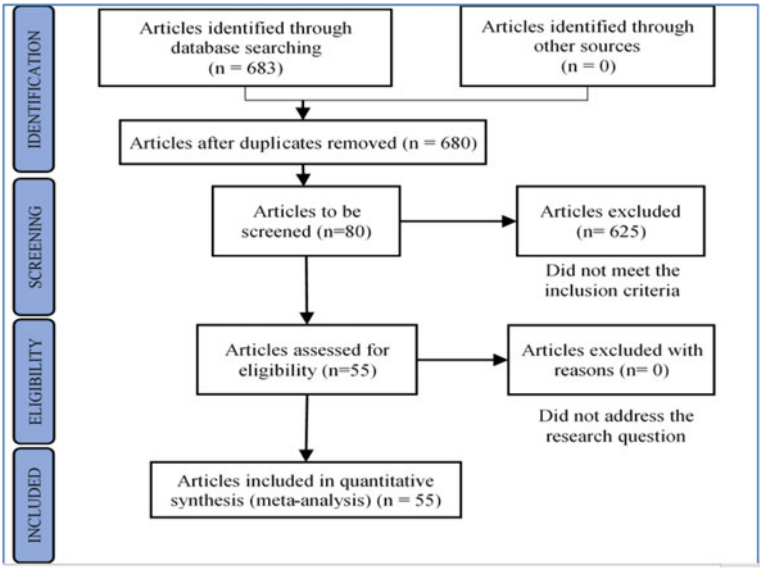

IDENTIFICATION
SCREENING
ELIGIBILITY
INCLUDED
Articles identified through database searching (n = 683)
Articles identified through other sources (n = 0)
Articles after duplicates removed (n = 680)
Articles to be screened (n=80)
Articles excluded (n= 625)
Did not meet the inclusion criteria
Articles assessed for eligibility (n=55)
Articles excluded with reasons (n= 0)
Did not address the research question
Articles included in quantitative synthesis (meta-analysis) (n = 55)

Fig. 2 Document inclusion and exclusion flowchart

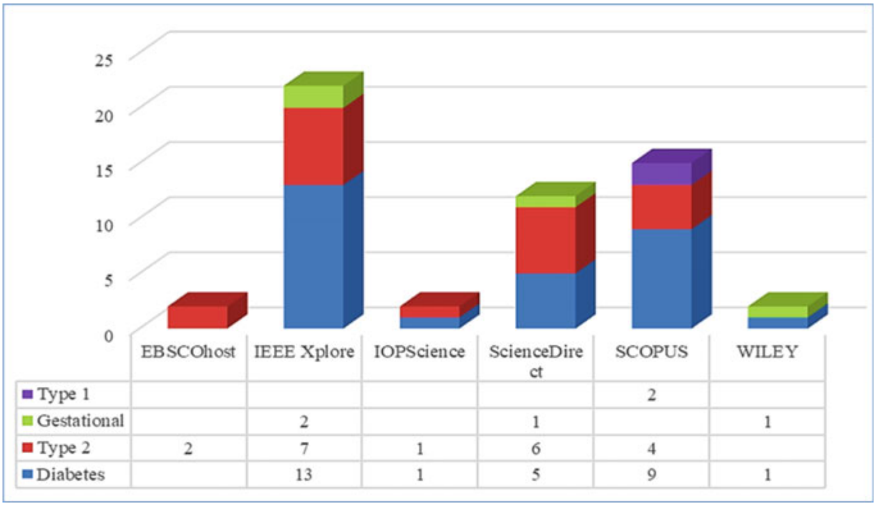
and which did not contribute to answering the research questions. This resulted in 55 articles for the systematic review in Fig. 2.

3 Results

Figure 3 represents the number of articles by database and type of diabetes.

Table 2 shows the categories of items according to the results found.

Figure 4 represents the number of articles by programming language used in the research, where the language.



	EBSCOhost	IEEE Xplore	IOPScience	ScienceDirect	SCOPUS	WILEY
🟪 Type 1					2	
🟩 Gestational		2		1		1
🟥 Type 2	2	7	1	6	4	
🟦 Diabetes		13	1	5	9	1

Fig. 3 Articles by database and type of diabetes

Table 2 Articles by type of diabetes

Categories	Articles
Type 1 diabetes mellitus	[6, 7]
Type 2 diabetes mellitus	[8–27]
Gestational diabetes mellitus	[2, 28–30]
Diabetes mellitus (type is not specified)	[1, 31–58]

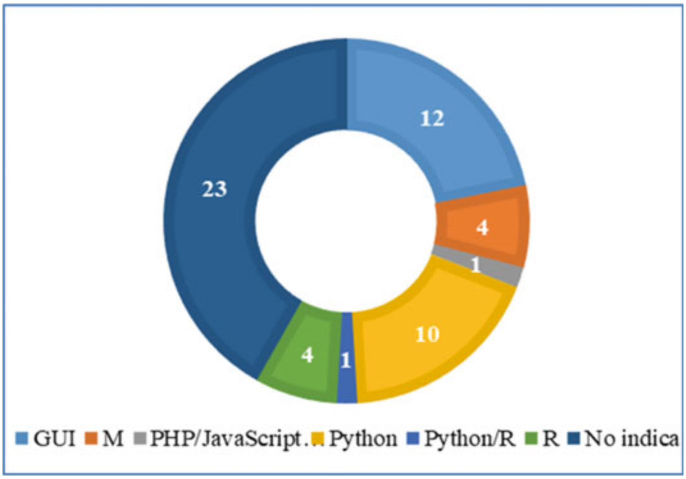


Fig. 4 Articles by programming language

4 Discussion

In this systematic investigation of the scientific literature, we analyze machine learning models for diabetes prediction and identify the best machine learning models, the most frequent implementation tools, as well as the largest amount of research according to the type of diabetes and countries, in order to answer the proposed questions:

RQ1. Which diabetes mellitus prediction models have shown the best results according to performance metrics over the past 4 years?
Figure 3 shows that most of the articles analyzed in this review use Accuracy as a metric to evaluate their models. The result obtained allows us to use this metric as a reference to identify the models with the best performance. According to references [7, 43, 45], it can be seen that the support vector machine, random forest and extreme learning machine models have obtained the best performance with 100%, 99% and 99% accuracy, respectively. It is important to mention that according to Fig. 4, it is shown that the support vector machine and random forest models are the models most used by researchers.

RQ2. Which tools and languages are the most widely used in the world to develop or implement machine learning models for diabetes mellitus prediction?
Although most of the researchers do not indicate the development environment of their models, a large number use the free software platform Weka as their modeling, visualization and data analysis tool, which is described by all the authors as a simple and intuitive tool that makes it much easier to carry out the aforementioned tasks. Furthermore, according to Fig. 4, it can be seen that graphical user interfaces (GUIs) are more used for modeling than the programming languages themselves. It is worth mentioning that according to references [7, 43, 45], the MATLAB tool, in which the M language is used, is the one with the highest accuracy (100%) when developing a machine learning model (support vector machine), followed by RStudio with the R language in which, when developing the random forest model, an accuracy of 99% was obtained.

RQ3: Which countries have the most research related to the prediction of diabetes mellitus been conducted in the last 4 years?
Figure 4 manifests that in the last four years (2018–2021), there is an increasing amount of research related to diabetes mellitus prediction; between 2019 and 2020, a great variety of publications were made especially in the IEEE Xplore databases followed by Scopus, and this result is supported by Fig. 3. This indicates that there is a preference by researchers to make their scientific publications related to diabetes prediction in the aforementioned databases.

All the articles analyzed in the present review come from the continents of Asia, North America, Europe and Africa (from highest to lowest). This result indicates that the development of machine learning models for the prediction of diabetes mellitus is a recurrent research topic almost all over the world. Also, it is shown that the vast majority of research is conducted in India followed by China. This result indicates that it is in these countries where there is more experience in the development of machine learning models for the prediction of diabetes mellitus; therefore, it is important to include research from the identified countries in future studies.

RQ4: What type of diabetes mellitus has had the highest amount of scientific research focused on prediction with machine learning worldwide?
According to Table 2, it can be seen that of all the articles analyzed in the present review, more research does not focus on a specific type of diabetes mellitus, but it can also be seen that there is a significant number of research that seeks to predict type 2 diabetes mellitus, and a small group focuses on gestational diabetes and type 1 diabetes. Figure 3 shows that, of all the articles analyzed, the vast majority of the research has used the PIMA Indian Diabetes dataset for training prediction models, and it is also observed that there is a minority that generates its own dataset. This result indicates that the information provided by this dataset is highly valued by researchers and is related to the fact that there is a greater amount of research on predictive models for type 2 diabetes and gestational diabetes because the variables in these data are identified as determinants for the prediction of the mentioned types.

5 Conclusions

The prediction models of diabetes mellitus that have presented better results in the last 4 years are support vector machine (100%), random forest (99%) and extreme learning machine (99%), according to Accuracy, which was defined as a metric to identify the best models due to its presence in most researches where they consider it as a determinant metric. The tools and languages with which machine learning models are usually developed or implemented worldwide are the free software platform Weka, for its ease of use, as well as MATLAB, in which the M language is used, followed by RStudio, these last two tools managed to develop models that obtained the highest scores according to Accuracy. Likewise, there is a greater number of studies that do not focus on a specific type of diabetes mellitus, but it is also observed that there is an important number of studies that seek to predict type 2 diabetes mellitus. Based on the results obtained, it is recommended for future research within the scope of this review, to work on the development of predictive models with the support vector machine algorithm due to the good results obtained, as well as to consider accuracy as a metric to evaluate model performance and to use MATLAB or RStudio as development tools.

References

1. Nnamoko N, Hussain A, England D (2018) Predicting diabetes onset: an ensemble supervised learning approach. IEEE Congr Evol Comput CEC 2018—Proc, pp 1–7 (2018). https://doi.org/10.1109/CEC.2018.8477663
2. Gnanadass I (2020) Prediction of gestational diabetes by machine learning algorithms. IEEE Potentials 39(6):32–37. https://doi.org/10.1109/MPOT.2020.3015190
3. Rippe JM (2021) The silent epidemic. Am J Med 134(2):164–165. https://doi.org/10.1016/j.amjmed.2020.09.028
4. WHO (2020) Recommendations for people living with NCDs, caregivers, family members and the public. World Heal Organ, pp 1–6. Available: https://apps.who.int/iris/handle/10665/331473
5. Mengist W, Soromessa T, Legese G (2020) Method for conducting systematic literature review and meta-analysis for environmental science research. MethodsX, **7**:100777. https://doi.org/10.1016/j.mex.2019.100777
6. Xue J, Min F, Ma F (2020) Research on diabetes prediction method based on machine learning. J Phys Conf Ser 1684(1). https://doi.org/10.1088/1742-6596/1684/1/012062
7. Cordelli E, Maulucci G, De Spirito M, Rizzi A, Pitocco D, Soda P (2018) A decision support system for type 1 diabetes mellitus diagnostics based on dual channel analysis of red blood cell membrane fluidity. Comput Methods Programs Biomed 162:263–271. https://doi.org/10.1016/j.cmpb.2018.05.025
8. Chatrati SP et al (2020) Smart home health monitoring system for predicting type 2 diabetes and hypertension. J King Saud Univ—Comput Inf Sci xxxx. https://doi.org/10.1016/j.jksuci.2020.01.010
9. Deberneh HM, Kim I (2021) Prediction of type 2 diabetes based on machine learning algorithm. Int J Environ Res Public Health 18(6):9–11. https://doi.org/10.3390/ijerph18063317
10. M. Tanvir Islam, M. Raihan, F. Farzana, P. Ghosh, and S. Ahmed Shaj: An empirical study on diabetes mellitus prediction using apriori algorithm. Adv. Intell. Syst. Comput., vol. 1166, pp. 539–550 (2021). doi: https://doi.org/10.1007/978-981-15-5148-2_48.
11. M. T. Islam, M. Raihan, F. Farzana, N. Aktar, P. Ghosh, and S. Kabiraj: Typical and Non-Typical Diabetes Disease Prediction using Random Forest Algorithm. 11th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2020, pp. 1–6 (2020). doi: https://doi.org/10.1109/ICCCNT49239.2020.9225430.
12. A. Mir and S. N. Dhage: Diabetes Disease Prediction Using Machine Learning on Big Data of Healthcare. Proc. - 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018, pp. 1–6 (2018). doi: https://doi.org/10.1109/ICCUBEA.2018.8697439.
13. R. Syed, R. K. Gupta, and N. Pathik: An Advance Tree Adaptive Data Classification for the Diabetes Disease Prediction. Int. Conf. Recent Innov. Electr. Electron. Commun. Eng. ICRIEECE 2018, pp. 1793–1798 (2018). doi: https://doi.org/10.1109/ICRIEECE44171.2018.9009180.
14. G. Tripathi and R. Kumar: Early Prediction of Diabetes Mellitus Using Machine Learning. ICRITO 2020 - IEEE 8th Int. Conf. Reliab. Infocom Technol. Optim. Trends Futur. Dir., pp. 1009–1014 (2020). doi: https://doi.org/10.1109/ICRITO48877.2020.9197832.
15. J. Beschi Raja, R. Anitha, R. Sujatha, V. Roopa, and S. Sam Peter: Diabetics prediction using gradient boosted classifier. Int. J. Eng. Adv. Technol., vol. 9, no. 1, pp. 3181–3183 (2019). doi: https://doi.org/10.35940/ijeat.A9898.109119.
16. Ebenzer PA, Bhattalwar R, Patel H, Kumar R (2019) Patient readmission prediction due to diabetes using machine learning classification. Int. J. Innov. Technol. Explor. Eng. 9(1):678–681. https://doi.org/10.35940/ijitee.A4561.119119
17. M. T. Student, K. Lakshmaih, E. Foundation, and G. District: Diabetic Prediction Using Kernel Based Support Vector Machine. vol. 9, no. 2, pp. 1178–1183 (2020).
18. M. S. Geetha Devasena, R. Kingsy Grace, and G. Gopu: PDD: Predictive diabetes diagnosis using datamining algorithms. Int. Conf. Comput. Commun. Informatics, ICCCI 2020, pp. 22–25 (2020). doi: https://doi.org/10.1109/ICCCI48352.2020.9104108.

19. V. L. Helen Josephine, A. P. Nirmala, and V. L. Alluri: Impact of Hidden Dense Layers in Convolutional Neural Network to enhance Performance of Classification Model. IOP Conf. Ser. Mater. Sci. Eng., vol. 1131, no. 1, p. 012007 (Apr. 2021). doi: https://doi.org/10.1088/1757-899X/1131/1/012007.
20. D. Jashwanth Reddy et al.: Predictive machine learning model for early detection and analysis of diabetes. Mater. Today Proc., no. xxxx (2020). doi: https://doi.org/10.1016/j.matpr.2020.09.522.
21. Tigga NP, Garg S (2020) Prediction of Type 2 Diabetes using Machine Learning Classification Methods. Procedia Comput. Sci. 167(2019):706–716. https://doi.org/10.1016/j.procs.2020.03.336
22. R. B. Lukmanto, Suharjito, A. Nugroho, and H. Akbar: Early detection of diabetes mellitus using feature selection and fuzzy support vector machine. Procedia Comput. Sci., vol. 157, pp. 46–54 (2019). doi: https://doi.org/10.1016/j.procs.2019.08.140.
23. L. Loku, B. Fetaji, and M. Fetaji: Prevention of Diabetes by Devising A Prediction Analytics Model. HORA 2020 - 2nd Int. Congr. Human-Computer Interact. Optim. Robot. Appl. Proc., pp. 1–4 (2020). doi: https://doi.org/10.1109/HORA49412.2020.9152894.
24. T. Mahboob Alam et al.: A model for early prediction of diabetes. Informatics Med. Unlocked, vol. 16, no. July, p. 100204 (2019). doi: https://doi.org/10.1016/j.imu.2019.100204.
25. R. Lee and C. Chitnis: Improving health-care systems by disease prediction. Proc. - 2018 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2018, pp. 726–731 (2018). doi: https://doi.org/10.1109/CSCI46756.2018.00145.
26. Kopitar L, Kocbek P, Cilar L, Sheikh A, Stiglic G (2020) Early detection of type 2 diabetes mellitus using machine learning-based prediction models. Sci Rep 10(1):1–12. https://doi.org/10.1038/s41598-020-68771-z
27. Khanam JJ, Foo SY (2021) A comparison of machine learning algorithms for diabetes prediction. ICT Express xxxx. https://doi.org/10.1016/j.icte.2021.02.004
28. H. Liu et al (2020) Machine learning risk score for prediction of gestational diabetes in early pregnancy in Tianjin, China. Diabetes Metab Res Rev (2020). https://doi.org/10.1002/dmrr.3397
29. Y. Srivastava, P. Khanna, and S. Kumar: Estimation of Gestational Diabetes Mellitus using Azure AI Services. Proc. - Amity Int. Conf. Artif. Intell. AICAI 2019, pp. 321–326 (2019). doi: https://doi.org/10.1109/AICAI.2019.8701307.
30. D. Sisodia and D. S. Sisodia: Prediction of Diabetes using Classification Algorithms. Procedia Comput. Sci., vol. 132, no. Iccids, pp. 1578–1585 (2018). doi: https://doi.org/10.1016/j.procs.2018.05.122.
31. Dey SK, Hossain A, Rahman MM (2019) Implementation of a web application to predict diabetes disease: an approach using machine learning algorithm. 21st Int Conf Comput Inf Technol ICCIT 2018, pp 1–5 (2019). https://doi.org/10.1109/ICCITECHN.2018.8631968
32. Li G, Liu Y, Li H, Yao R, Li C (2021) MCMC impute missing values and Bayesian variable selection for logistic regression model to predict Pima Indian Diabetes. J Phys Conf Ser 1865(4):042087. https://doi.org/10.1088/1742-6596/1865/4/042087
33. C. Zhu, C. U. Idemudia, and W. Feng: Improved logistic regression model for diabetes prediction by integrating PCA and K-means techniques. Informatics Med. Unlocked, vol. 17, no. April, p. 100179 (2019). doi: https://doi.org/10.1016/j.imu.2019.100179.
34. K. L. Priya, M. S. Charan Reddy Kypa, M. M. Sudhan Reddy, and G. R. Mohan Reddy: A Novel Approach to Predict Diabetes by Using Naive Bayes Classifier. Proc. 4th Int. Conf. Trends Electron. Informatics, ICOEI 2020, no. Icoei, pp. 603–607 (2020). doi: https://doi.org/10.1109/ICOEI48184.2020.9142959.
35. R. S. Raj, D. S. Sanjay, M. Kusuma, and S. Sampath: Comparison of Support Vector Machine and Naïve Bayes Classifiers for Predicting Diabetes. 1st Int. Conf. Adv. Technol. Intell. Control. Environ. Comput. Commun. Eng. ICATIECE 2019, pp. 41–45 (2019). doi: https://doi.org/10.1109/ICATIECE45860.2019.9063792.
36. D. Vigneswari, N. K. Kumar, V. Ganesh Raj, A. Gugan, and S. R. Vikash: Machine Learning Tree Classifiers in Predicting Diabetes Mellitus. 5th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2019, pp. 84–87 (2019). doi: https://doi.org/10.1109/ICACCS.2019.8728388.

37. S. C. Gupta and N. Goel: Performance enhancement of diabetes prediction by finding optimum K for KNN classifier with feature selection method. Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020, no. Icssit, pp. 980–986 (2020). doi: https://doi.org/10.1109/ICSSIT48917.2020.9214129.
38. P. S. Kohli and A. L. Regression: Application of Machine Learning in Disease Prediction. IEEE 5th Int. Conf. Comput. Commun. Autom. ICCCA 2020, pp. 1–4 (2020).
39. P. Kaur, N. Sharma, A. Singh, and B. Gill, "CI-DPF: A Cloud IoT based Framework for Diabetes Prediction," 2018 IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2018, pp. 654–660, 2019, doi: https://doi.org/10.1109/IEMCON.2018.8614775.
40. Karthikeyan S. M, C. P.J, G. C. B, and M. J: Performance Analysis Based on Data Mining Technique in Predicting the Diabetic Disease – Decision tree and Naïve Bayes. 1st Int. Conf. Adv. Inf. Technol., pp. 2019–2022 (2019).
41. S. Thenappan, M. Valan Rajkumar, and P. S. Manoharan: Predicting Diabetes Mellitus Using Modified Support Vector Machine with Cloud Security. IETE J. Res., pp. 1–11 (2020). doi: https://doi.org/10.1080/03772063.2020.1782781.
42. Patil R, Tamane S (2018) A comparative analysis on the evaluation of classification algorithms in the prediction of diabetes. Int. J. Electr. Comput. Eng. 8(5):3966–3975. https://doi.org/10.11591/ijece.v8i5.pp3966-3975
43. Suvarnamukhi B, Seshashayee M (2019) Big data processing system for diabetes prediction using machine learning technique. Int. J. Innov. Technol. Explor. Eng. 8(12):4478–4483. https://doi.org/10.35940/ijitee.L3515.1081219
44. Franklin RG, Muthukumar B (2020) Detection of diabetes mellitus using machine learning algorithms. Int. J. Res. Pharm. Sci. 11(4):6881–6887. https://doi.org/10.26452/ijrps.v11i4.3662
45. P. S. Kumar and S. Pranavi: Performance analysis of machine learning algorithms on diabetes dataset using big data analytics. Int. Conf. Infocom Technol. Unmanned Syst. Trends Futur. Dir. ICTUS 2017, vol. 2018-Janua, no. Iddm, pp. 508–513 (2018). doi: https://doi.org/10.1109/ICTUS.2017.8286062.
46. Pandeeswary P, Janaki M (2019) Performance analysis of big data classification techniques on diabetes prediction. Int. J. Innov. Technol. Explor. Eng. 8(10):533–537. https://doi.org/10.35940/ijitee.J8840.0881019
47. S. Raghavendra and J. Santosh Kumar: Performance evaluation of random forest with feature selection methods in prediction of diabetes. Int. J. Electr. Comput. Eng., vol. 10, no. 1, pp. 353–359 (2020). doi: https://doi.org/10.11591/ijece.v10i1.pp353-359.
48. S. C. Gupta and N. Goel: Enhancement of Performance of K-Nearest Neighbors Classifiers for the Prediction of Diabetes Using Feature Selection Method. IEEE 5th Int. Conf. Comput. Commun. Autom. ICCCA 2020, pp. 681–686 (2020). doi: https://doi.org/10.1109/ICCCA49541.2020.9250887.
49. Mujumdar A, Vaidehi V (2019) Diabetes Prediction using Machine Learning Algorithms. Procedia Comput. Sci. 165:292–299. https://doi.org/10.1016/j.procs.2020.01.047
50. Samant P, Agarwal R (2018) Machine learning techniques for medical diagnosis of diabetes using iris images. Comput Methods Programs Biomed 157:121–128. https://doi.org/10.1016/j.cmpb.2018.01.004
51. B. Jain, N. Ranawat, P. Chittora, P. Chakrabarti, and S. Poddar: A machine learning perspective: To analyze diabetes," Mater. Today Proc., no. xxxx (2021). doi: https://doi.org/10.1016/j.matpr.2020.12.445.
52. M. Radja and A. W. R. Emanuel: Performance Evaluation of Supervised Machine Learning Algorithms Using Different Data Set Sizes for Diabetes Prediction. Proceeding - 5th Int. Conf. Sci. Inf. Technol. Embrac. Ind. 4.0 Towar. Innov. Cyber Phys. Syst. ICSITech 2019, pp. 252–258 (2019). doi: https://doi.org/10.1109/ICSITech46713.2019.8987479.
53. R. Aminah and A. H. Saputro: Diabetes prediction system based on iridology using machine learning. 6th Int. Conf. Inf. Technol. Comput. Electr. Eng. ICITACEE 2019, pp. 1–6 (2019). doi: https://doi.org/10.1109/ICITACEE.2019.8904125.
54. Cahn A et al (2020) Prediction of progression from pre-diabetes to diabetes: Development and validation of a machine learning model. Diabetes Metab Res Rev 36(2):1–8. https://doi.org/10.1002/dmrr.3252

55. T. Nibareke and J. Laassiri: Using Big Data-machine learning models for diabetes prediction and flight delays analytics. J. Big Data, vol. 7, no. 1, (2020). doi: https://doi.org/10.1186/s40537-020-00355-0.
56. Viloria A, Herazo-Beltran Y, Cabrera D, Pineda OB (2020) Diabetes Diagnostic Prediction Using Vector Support Machines. Procedia Comput. Sci. 170:376–381. https://doi.org/10.1016/j.procs.2020.03.065
57. R. Deo and S. Panigrahi: Performance Assessment of Machine Learning Based Models for Diabetes Prediction. IEEE Healthc. Innov. Point Care Technol. HI-POCT 2019, pp. 147–150 (2019). doi: https://doi.org/10.1109/HI-POCT45284.2019.8962811.
58. J. Ma: Machine Learning in Predicting Diabetes in the Early Stage. Proc. - 2nd Int. Conf. Mach. Learn. Big Data Bus. Intell. MLBDBI 2020, pp. 167–172 (2020). doi: https://doi.org/10.1109/MLBDBI51377.2020.00037.

Industrial Pumps Anomaly Detection and Semi-supervised Anomalies Labeling Through a Cascaded Clustering Approach

Qiang Duan, Zhihang Jiang, Wei Li, Kai Jiang, Weiduo Jin, Ling Yu, Mengmeng Jiang, Jing Zhao, Rui Li, and Hui Zhang

Abstract Automation technology has brought significant changes to agriculture, industry, commerce and other fields, among which the machine learning algorithms are the important applications of predictive maintenance of industrial equipment. In general, anomalous trends should be detected timely before failure occurs so that unscheduled downtime can be avoided. In addition, predictive maintenance can avoid unnecessary maintenance and make good use of component remaining life by setting appropriate maintenance periods for worn parts. In this paper, based on the real case in which data collected by the various sensors on coal mine pumping system, we propose a cascaded unsupervised clustering method that consists of DBSCAN and spectral clustering to identify uncommon abnormal data and classify the common abnormal data. As equipment continuously operating, the proposed cascaded clustering method can gradually utilize the obtained uncommon abnormal data to enlarge the common abnormal data. This process implemented through periodic manually labeling is regarded as a semi-supervised manner. The results show that DBSCAN has good discriminative power for uncommon abnormal data, and the spectral clustering can properly classify working condition of water pumps with 93% accuracy on test data.

Keywords Anomaly detection · Clustering · DBSCAN · Machine learning · Spectral clustering

Qiang Duan, Zhihang Jiang, Wei Li: contributed equally to this study.

Q. Duan · Z. Jiang · W. Li · K. Jiang · L. Yu · M. Jiang · R. Li · H. Zhang (✉)
Inspur Academy of Science and Technology, Jinan, Shandong, China
e-mail: zhanghui@inspur.com

W. Jin
Inspur International Limited, Jinan, Shandong, China

J. Zhao
Shandong Yingxin Computer Technology Co., Ltd., Jinan, China

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_31

1 Introduction

Anomaly detection can measure machine operation parameters collected by various sensors to predict the possibility of machine failure. It needs comprehensive information about machine statues for physical metering, process modeling or data-driven methods. Generally, it is more efficient to apply data-driven method in this area. Benefited from the application of sensors and data-driven methods in anomaly detection, the equipment failure monitoring is more predictive instead of preventive [5].

Industrial pumps play an import role in many industrial scenes. They require proper maintenance to keep normal working state and extend lifespan. In order to avoid sudden malfunction or unnecessary maintenance, the machine learning is used for anomaly detection and predictive maintenance. The ratio of machine learning application in industrial sectors was going up to 65% in 2018, which is continuously increasing [6].

There are two major categories of available algorithm for anomaly detection: supervised algorithm for labeled data and unsupervised algorithm for unlabeled data. For the first kind, they use labeled anomaly data to train a classification model, such as SVM, logistic regression and decision tree. [7]. However, the real-world industrial problem is unlikely to have large amount of data to build a decent machine learning model. Due to the machine failure is relatively rare situation, the collected data has very small percentage of anomalies. For the second kind, they use unlabeled data to train a regression model or clustering model, such as one-class-SVM, density estimation and isolation forest. [7] These algorithms are generally based on distance, density, statistics intrinsic features of data rather than labels. So that the model can be built by an unsupervised manner.

In this paper, we propose a cascaded unsupervised clustering method that consists of DBSCAN [5] and spectral clustering [11] to identify uncommon abnormal data and classify the common abnormal data. As equipment continuously operates, proposed cascaded clustering method can gradually utilize the obtained uncommon abnormal data to enlarge the common abnormal data through periodic manually labeling that implements a semi-supervised data labeling. The uncommon abnormal data is the failure situation that rarely occurred in the past pump operation, which is processed by DBSCAN to separate from other normal data. And the common abnormal data is the frequently occurred situation, which can be clustered well by spectral clustering.

This paper is organized as follows: The instruction is followed by related works. The third section presents the preliminary knowledge on two clustering algorithms and the main idea of the proposed cascaded method. The experimental results on the test dataset are shown in next section, along with datasets explanation and results discussion. Finally, conclusions are drawn in the last section.

2 Related Work

Classic anomaly detection techniques are based on continuously device condition monitoring, such as inspecting the output of physical sensors, leaks and audible noise [1]. Benefited from the booming development of communication technology and cloud computing technology, the remote device condition monitoring is broadly implemented to realize real-time anomaly detection [10]. In addition, it is feasible to predict remaining life of components by applying data-driven methods like time-series decomposition, regression, long short-term memory neural network, etc., which is related to anomaly detection as well.

For the supervised anomaly detection, it uses normal operation data as training data. One approach uses graphs for modeling abnormal data, while another uses principal component classifiers to build models [13]. The anomaly detection in more difficult scene tends to use deep learning approach since it has more representative ability to deal with high-dimensional or large-scale data [4]. Nabanita etc. [3] used supervised classification method to reach about 80 % accuracy.

For unsupervised anomaly detection, the operation information is available, but no related label indicating component remaining life or anomalies. The lack of labels is the most common situation in industrial anomaly detection [14]. Since an anomaly is an outlier pattern that differs from the expected behavior, a simple approach is to find the data which is far away from normal data-defined boundary [2]. The boundary can be obtained by clustering.

There are various clustering techniques, such as partitioning clustering, hierarchical clustering and density-based clustering. Density-based spatial clustering of applications with noise (DBSCAN) is one of the widely used density-based clustering algorithms. The main principle of DBSCAN in outlier detection is to define a cluster that contains a minimum number of points in the specified radius [5]. Spectral clustering is another popular and efficient clustering method. It allows to find clusters even of very irregular shapes. In 2012, Lucinska et al. improved the spectral clustering method and achieved better performance in practical applications [8].

Algorithm 1: DBSCAN

```
1 Set $t = 1$
2 Use $\varepsilon$ and MinPts to find an unclassified core point p and add it to the set $C_t$
3 Find all the unclassified points in the $\varepsilon$-neighborhood and add them to the set F
4 Get a point q in F and mark q to be classified, assign q to the cluster $C_t$ , and remove q from
  the set F
5 Check if q is a core point, if so, add all the unclassified points in the $\varepsilon$-neighborhood to the
  set F
6 Repeat steps 4 and 5 until the set of seeds is empty.
7 Set $t = t + 1$ and repeat steps 2–5 until no more core points can be found.
8 Output all the clusters; and mark all the points which do not belong to any cluster as noise
```

3 Methods

3.1 Density-Based Spatial Clustering of Applications with Noise (DBSCAN)

DBSCAN is a widely used clustering algorithm in machine learning [12]. It defines a cluster as the largest set of densely connected samples derived from the density reachability relation. Given a Dataset $D = \{x_1, x_2, ..., x_m\}$, distance ε and minimum elements MinPts, the process of DBSCAN is as follows:

3.2 Spectral Clustering

We use spectral clustering to identify pump operation status [9] .Given a Dataset $D = \{x_1, x_2, \ldots, x_m\}$, the process of spectral clustering is as follows:

Algorithm 2: Spectral clustering

```
Using Euclidean distance to find k symmetric nearest neighbors of each point
For each two vertices $x_i$ and $x_j$, the connecting edge $v_{ij}$ is created if vertex $x_i$ belongs to
  k-nearest neighbors of vertex $x_j$ and vice versa
Constructed the adjacency matrix A, $a_{ij}$ is set to one if and only if there is an edge joining
  the two vertices; otherwise, $a_{ij}$ equals 0. Also, all diagonal elements of the affinity matrix A
  are zero
Create the diagonal matrix D and calculate Signless Laplace matrix M
Compute top w eigenvectors of M and determine overlapping eigenvectors (related to the
  same cluster)
Calculate modularity Q corresponding to the graph cut for each overlapping eigenvector and
  choose the best one
Create a set of eigenvectors A and assign each point x to one eigenvector from the set A,
  having the biggest entry for x
```

3.3 Cascaded Usage of Two Clustering Methods

We cascade the pump operation data using two algorithms, DBSCAN and spectral clustering, to both identify rare anomalies and categorize common anomalies. Most importantly, we can collect and process the obtained anomaly data as the equipment continuously operates, then achieve semi-supervised anomaly status identification or anomaly data labeling by periodic manual marking. The specific process is as follows, which is also shown in Fig. 1.

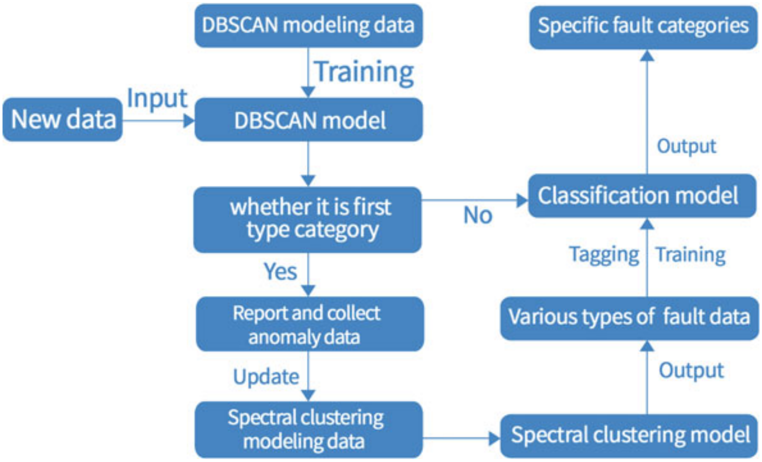

DBSCAN modeling data
Training
New data
Input
DBSCAN model
whether it is first type category
No
Yes
Report and collect anomaly data
Update
Spectral clustering modeling data
Spectral clustering model
Output
Various types of fault data
Tagging
Training
Classification model
Output
Specific fault categories

Fig. 1 The workflow of the proposed method

First of all, we divide the pump abnormality into two categories, one is the failure that has never occurred or rarely occurred during the historical operation of the pump. The other is the failure that occurs several times in the historical data, which has more abnormal data. For these two cases, we use different algorithms to handle.

For the first type of pump abnormality, among the commonly used anomaly detection methods, such as k-means clustering and Gaussian mixture model, they require a prior given number of clusters that do not meet the needs of the study. For methods that do not require a prior given number of clusters, we found that DNSCAN has better performance in pump anomaly detection comparing to isolated forest, OPTICS and DBSCAN methods. Figure 2 shows the performance of the three methods on pump anomaly detection with positive pressure as an example. So we choose the DBSCAN algorithm to detect the first type of anomaly. We train the machine learning model using a small amount of exception data and a large amount of normal operation data. Then, we deploy the model to the corresponding device. When new data is passed to the model, DBSCAN can identify the fault and report to the user side if it is the first type of abnormal data. Furthermore, the reported exception data is saved for later use.

Using the DBSCAN algorithm only is not sufficient, and it is difficult to achieve the desired results with DBSCAN when the incoming anomalous data is a large percentage of the total incoming data. For the second category of anomalies, we also compared a variety of clustering algorithms. Finally, we found that the spectral clustering algorithm can more accurately identify the operating status of the pump and better distinguish between various types of faults and normal operating status. Therefore, we use the spectral clustering algorithm as a supplement to deal with the second category of anomalies. After training the model, when DBSCAN fails to detect anomalies, we continue to substitute the data into the spectral clustering

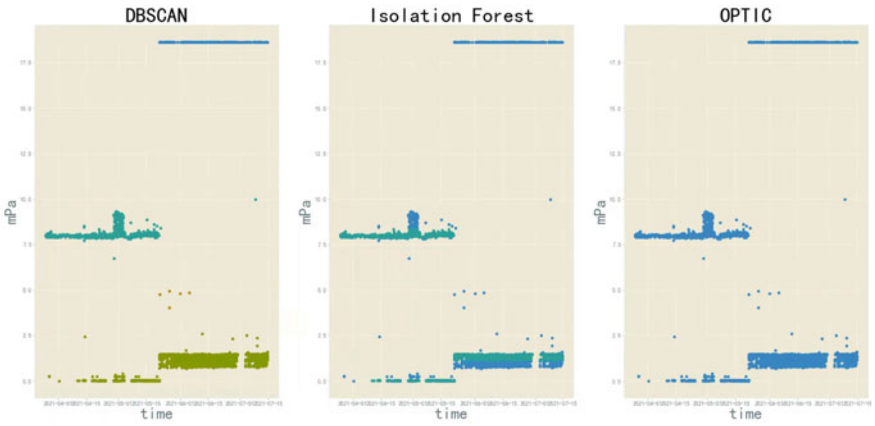


Fig. 2 The comparison of three methods using positive pressure for example

model, which can distinguish the incoming data into a specific type of fault or normal operation state so that we can proceed to the next step.

Using manual identification and labeling of various types of different data output from spectral clustering, these data are processed and used as a training set for a classification model, which can be constructed using random forests or other classification algorithms. Consequently, we turn the clustering problem into a classification problem.

When new data comes in, we first use DBSCAN to determine if it is a Type 1 error. If so, we can identify the data and save for manually labeling. Otherwise, it is passed to the classification model to determine whether it is an anomaly or normal condition.

After a period of operation, we can pass the anomaly data collected by DBSCAN into the spectral clustering model for training. If a new class is generated, then it means that there is a new class of faults, and we then use manual methods to discern exactly which class of faults is. Then, labeling the anomaly data to create a new class of faults. After enough time, when new data collection is ready to train a model, we update the classification model by substituting the new fault data into the classification model training set.

4 Experimental Results

4.1 Dataset

The dataset is collected from a certain coal mine enterprise with several industrial pumps for draining cooling water. In this paper, we mainly use No. 2 water pump

Table 1 Description of continuous variables

Name	Num. valid value	Average	Variance
PP	841,223	6.16	42.59
NP	839,252	36.25	3308.42
PAV	833,456	10,207.52	34,668.31
PAC	475,957	87.28	1587.17
HV	844,739	0.39	0.16
VV	809,543	0.34	0.11
ST	781,243	77.81	173.92
PFAT	786,059	37.53	31.05
PRAT	790,149	38.82	10.40
MFAT	803,888	68.24	290.28
MRAT	792,695	59.21	109.34
PMECO	158,526	43.85	2462.23
PF	180,113	136.60	15,649.57

in central pump room. It used sensors to monitor the water pump from 03-25-2021 18:22:47 to 14-07-2021 19:30:58 and recorded the various kinds of data about the water pump. In addition, the dataset includes 13 continuous variables and 15 binary variables. The continuous variables are *Positive Pressure (PP), Negative Pressure (NP), Phase A voltage (PAV), Phase A Current (PAC), Horizontal Vibration (HV), Vertical Vibration (VV), Stator Temperature (ST), Pump Front Axle Temperature (PFAT), Pump Rear Axle Temperature (PRAT), Motor Front Axle Temperature (MFAT), Motor Rear Axle Temperature (MRAT), Percent of Main Electric Value Opened (PMECO), Pump Flow (PF)*. The binary variables are *Main Electric Valve Open (MEVO), Main Electric Valve Close (MEVC), Operating Status(OS), No.1 valve Open(N1VO), No.1 valve Close (N1VC), No.2 valve Open (N2VO), No.2 valve Close, No.3 valve Open (N3VO), No.3 valve Close (N3VC), Fully Automatic Control (FAC), Semi Automatic Control (SAC), Manual Control (MC), Remotely Control (RC), Local (L), Inspect (I)*. Table 1 indicates the amount of data after deleting the missing data, average and variance for every continuous variable. Similarly, Table 2 shows the amount of data after deleting the missing data and the ratio of 1 for every variable.

Based on the tables above, some variables are not necessary for detecting malfunction, since they are equal to 0 all the time. Furthermore, some variables are highly correlated. For example, the correlation between MEVO and MEVC is almost -1 and the correlation between MEVO and OS is almost 1. Moreover, both PMECO and MEVO measure the how much the main electric value opens, so it is not necessary to use all the variables to build model. Finally, we chose to keep all the continuous variables and RC,L,R to detect the malfunction. Besides, the range of these variables is different from each other, which could affect the result of clustering. Thus, the normalization was implemented to transform the variable into range from 0 to 1.

Table 2 Description of binary variables

Name	Num. valid value	Ratio of 1
MEVO	162,110	0.43
MEVC	162,180	0.54
OS	159,921	0.46
N1VO	154,446	0
N2VO	156,791	0
N3VO	157,428	0
N1VC	153,651	0
N2VC	155,324	6×10^{-6}
N3VC	154,145	0
FAC	144,609	0
SAC	143,871	0
MC	142,979	0
RC	143,414	0.88
L	141397	0.0014
I	146129	0.095

4.2 Detected First Type Error

The property of first type error is that they are far away from the rest data, which means that the method we used should be sensitive to the isolated data. Also, since it is difficult to find how the malfunction data distributed in the space spanned by the variables, it would be better to use a clustering method without setting the number of clusters should be separated in advance. By comparing the performance of different methods, DBSCAN is more suitable than other clustering methods in this scenario. When implementing the DBSCAN method, it requests large memory by running the whole algorithm on all variables, so DBSCAN is implemented to each variable independently. In addition, there is no need for normalizing the dataset. Furthermore, performance of DBSCAN is highly relevant to the choice of MinPts. To guarantee that the DBSCAN method can detect most of the malfunction points and is not too sensitive to the normal data, MinPts is carefully selected based on the results of DBSCAN. Figure 3 shows the DBSCAN results that are constructed by random selected 10,000 data points for each continuous variables, and different colors represent the different clusters. In these figures, it is obvious that there are some points far away from the others, and we recognize them as the malfunction points. For example, the green-yellow points in Phase A Current, the green-yellow and green-blue points in Phase A Voltage, the brown points in the positive pressure and the green-yellow and green-blue points in the negative pressure. In the figure of temperature, there is no obvious malfunction points. For the figure of vibration, there is one malfunction point in vertical vibration.

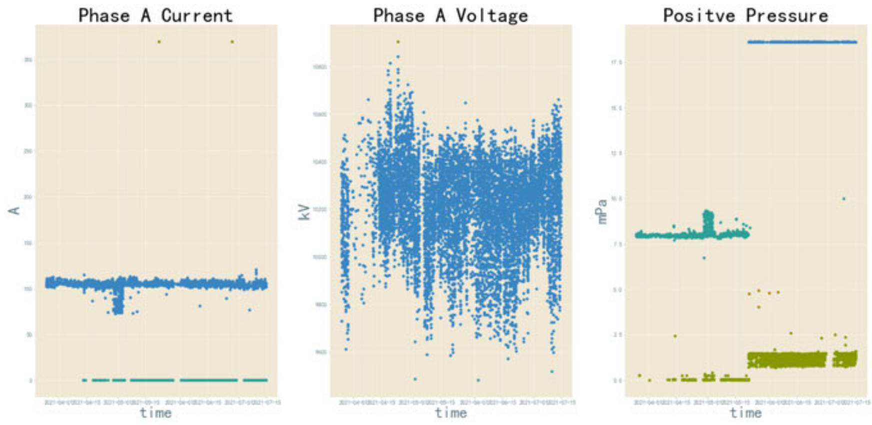


Fig. 3 The result of DBSCAN

4.3 Detected Second Type Error

To find the second type error, we implemented spectral clustering, which has a better performance than other clustering methods. After comparing the clustering results with different parameters, the result of spectral clustering based on the 300-Nearest Neighbor Graph is the closest to the facts. In this paper, we chose the data from 20-05-2021 18:08:13 to 22-05-2021 20:59:15 and from 30-06-2021 00:09:49 to 30-06-2021 13:18:35 to run spectral clustering method. The reason why we chose these data was that this data contains all the working status of water pump. By trying the preset number of clusters to be equal 2 through 10, the best result appeared under number of clusters was equal to 7. In this setting, the 7 clusters separated by spectral clustering could approximately match the 7 work status for the water pump. The result is shown in Fig. 4. Color 0 represents the water pump was working and remotely controlled, colors 1 and 2 represent the pump was just turned off and remotely controlled, color 3 represents the water pump was working but there could be some obstructions in the pump, color 4 represents the water pump was not working and not remotely controlled, color 5 represents the negative pressure was abnormal, and color 6 represents the water pump was working and not remotely controlled. The data labeled color 3 and 5 is the malfunction data.

These data labeled by spectral clustering can be used to build classification model. For convenience, we merge the class 1 and class 2, because both of them represent the same working status. Furthermore, we constructed a test dataset by selecting data that was not used to build model and manually labeled these data. By comparing results of KNN, SVM, random forest, LDA, logistic regression model, the random forest has the highest accuracy which is about 0.93.

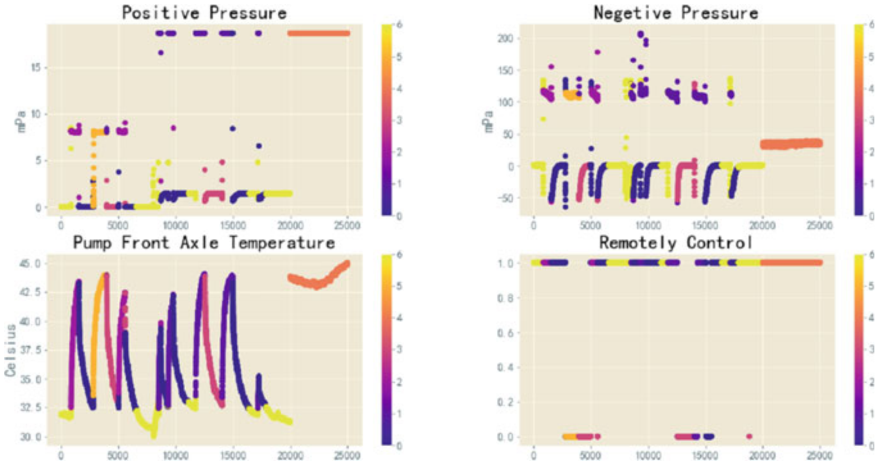


Fig. 4 The result of spectral clustering

5 Conclusions

The present study proposed a cascaded clustering method consisting of DBSCAN and spectral clustering, which is used to deal with anomaly detection problem in a real-world industrial dataset. The proposed method is verified on two kinds of data: rarely occurred abnormal data and commonly occurred abnormal data. Using DBSCAN on the first type of data can properly distinguish the small amount of anomalies. And using spectral clustering on general abnormal data can properly cluster same type of data into identical cluster. After a period operation of DBSCAN, the collected data can be labeled and fed to the spectral clustering model for updating model. Consequently, with manually labeling the output cluster of spectral clustering, a semi-supervised anomaly detection and classification method is implemented.

References

1. Babu GS, Chittaranjan Das V (2013) Condition monitoring and vibration analysis of boiler feed pump. Int J Sci Res Publ 3(6):1–7
2. Chandola V, Banerjee A, Kumar V (2009) Anomaly detection: a survey. ACM Comput Surv (CSUR) 41(3):1–58
3. Dutta N, Kaliannan P, Subramaniam U (2021) Application of machine learning algorithm for anomaly detection for industrial pumps. In: Machine learning algorithms for industrial applications. Springer, pp 237–263
4. Erfani SM, Rajasegarar S, Karunasekera S, Leckie C (2016) High-dimensional and large-scale anomaly detection using a linear one-class svm with deep learning. Pattern Recogn 58:121–134
5. Ester M, Kriegel H-P, Sander J, Xu X et al (1996) A density-based algorithm for discovering clusters in large spatial databases with noise. KDD 96:226–231

6. Larrañaga P, Atienza D, Diaz-Rozo J, Ogbechie A, Puerto-Santana C, Bielza C (2018) Industrial applications of machine learning. CRC Press
7. Leung K, Leckie C (2005) Unsupervised anomaly detection in network intrusion detection using clusters. Proceedings of the twenty-eighth Australasian conference on computer science 38:333–342
8. Lucińska M, Wierzchoń ST (2012) Spectral clustering based on k-nearest neighbor graph. In: IFIP international conference on computer information systems and industrial management. Springer, pp 254–265
9. Lucinska M, Wierzchon ST (2012) Spectral clustering based on k-nearest neighbor graph. In: CISIM
10. Moleda M, Momot A, Mrozek D (2020) Predictive maintenance of boiler feed water pumps using scada data. Sensors 20(2):571
11. Ng AY, Jordan MI, Weiss Y (2002) On spectral clustering: analysis and an algorithm. In: Advances in neural information processing systems, pp 849–856
12. Sander J, Ester M, Kriegel H-P, Xu X (2004) Density-based clustering in spatial databases: the algorithm gdbscan and its applications. Data Min Knowl Disc 2:169–194
13. Shyu M-L, Chen S-C, Sarinnapakorn K, Chang LW (2003) A novel anomaly detection scheme based on principal component classifier. Technical report, Miami Univ Coral Gables Fl Dept of Electrical and Computer Engineering
14. Syarif I, Prugel-Bennett A, Wills G (2012) Unsupervised clustering approach for network anomaly detection. In: International conference on networked digital technologies. Springer, pp 135–145

Is It Citizen-Centric? A Tool for Evaluating E-government Websites' Citizen-Centricity

Kamalia Azma Kamaruddin and Nur Jannah Johari

Abstract A citizen-centric e-government website is an important component for today's governments because it is a significant instrument for increasing access to and from citizens. Evaluation of citizen-centric e-government websites content deserves attention, and a tool that focuses on evaluating e-government websites that provide a checklist of important citizen-centric characteristics is needed for e-government practitioners. This paper aims to develop an evaluation tool to measure citizen-centricity in e-government websites and demonstrate the application of this tool in Malaysia e-government websites. Using qualitative methods of literature analysis and website observation, four components and thirty-nine characteristics in seven themes were identified and incorporated into a tool named Citizen-centric Checklist for E-Government Website (CCEW). This assessment tool provides a checklist of citizen-centric characteristics that should be present in the content of e-government websites. It is designed to be a guideline for evaluators of e-government websites from government or external agencies mandated to perform e-government websites evaluation. To demonstrate the tool, CCEW is employed into Malaysia's 5-stars e-government websites to identify its citizen-centricity level.

Keywords Citizen-centric · E-government · Websites evaluation · Evaluation tool

1 Introduction

Through rapid and significant development in information and communication technology, e-government services have greatly facilitated governments' agencies worldwide to provide beneficent services to the citizens efficiently [1]. In line with this technological change, governments have shifted its focus toward the citizens as the main part of e-government strategies, called customer-focus or citizen-centric. Meeting the demands of citizens is fundamental to the present-day view of citizen-centric service delivery [2]. Thus, providing citizen-centric websites in e-government can

K. A. Kamaruddin (✉) · N. J. Johari
Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, Malaysia
e-mail: kamalia@fskm.uitm.edu.my

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_32

be considered as a crucial element for any modern governments. Kamau et al. [3] stated that e-government websites' achievement is measured by how well the citizens have accepted it.

Understanding the requirements and expectations of citizen is the primary objective in citizen-centricity where it views the government from outside-in before designing public services and policies [4]. Citizen-centric government service delivery is a concept which place citizens in the middle while providing a one-stop channel for them to access all the services that they need [1]. This approach will significantly increase efficiency and reduce bureaucracy in government offices [5]. Thus, there is a need to perform evaluation on e-government websites through the lens of citizen-centricity which is vital to the adoption of e-government services [1].

There have been many models and frameworks in literatures that evaluate e-government websites using diverse approaches [1, 2, 6–9], but they provide limited consideration of building a practical instrument to assess e-government websites using the citizen-centric approach. Thus, evaluation of citizen-centric e-government websites content deserves attention. Particularly, the evaluation should be aligned with citizens' needs and preferences in websites use so the acceptance and use of web-based services can be maximized [9]. On the other hand, Kamaruddin and Noor [10] have developed a citizen-centric demand model and suggested an assessment tool to evaluate citizen-centricity in e-government websites to be developed as extension of their work. Due to the above reasons, this research will identify the characteristics of citizen-centric e-government websites and develop an evaluation tool to measure it. Finally, this research will demonstrate the usage of the tool by performing an evaluation of Malaysia e-government websites' content.

2 Related Works

Generally, e-government can be defined as "government's use of ICT, particularly, web-based applications, to enhance the access to and delivery of government information and services to citizens, businesses, employees and other agencies and entities" [11]. It is common for the present government particularly in the developed countries to work using ICT to reach and serve their citizens. By putting the citizens at the center of any government's initiatives, terms such as "citizen-centric", "citizen-focused" or "citizen-oriented" have been widely used to refer to the state. Citizen-centric e-government means looking into government service delivery through citizens' perspective where their needs and expectations are the primary concerns [12]. Misra [13] suggested that for any electronic intervention qualified to be called citizen-centric e-government, it must meet twenty criteria that had been proposed. In addition to that, Zibret et al. [14] have summarized seven characteristics of a citizen-centric government which consists of multiple behavioral elements. Although varied in focus, the core of citizen-centricity mostly belongs in the aspect of e-governments' design and delivery. Citizen-centric e-government service gave better realization of what are the citizens' needs; thus, reassessment of e-government evaluation approaches to citizen-based is clearly an imperative thing to do [1].

It is important to evaluate web-based e-government services as the taxpayer money spent on developing it should provide return of value over time [15]. Various past literatures concerned on the e-government website quality evaluation have resulted in the emergence of many models regarding the evaluation. For instance, Osman et al. [8] suggested the implementation of Information, e-Service and Organization (IEO) Tasks Model to evaluate public sector's websites functionality. On the other hand, Misra [13] has proposed similar criteria used in the US e-government websites evaluation for the assessment of official Indian websites which consists of 25 features and grouped into 7 indexes of services. Zahran et al. [16] suggested a more comprehensive evaluation that considered the front-office and other factors, while Eschenfelder and Miller [17] have developed a framework that assesses text information in government agency website tool to evaluate government websites, but they were focusing only on its textual information content.

The United Nations' E-Government Development Index (UN-EGDI) is based on expert assessment of online presence of all UN member states, which evaluates national portals and websites and how public policies and strategies were implemented in the delivery of key services [18]. On the other hand, Waseda University's study has broader measurement indicators that cover network infrastructure and organizational structure of the countries under scrutiny [19]. Waseda e-government ranking is based on ten indicators which included thirty-five sub-indicators and 154 questions. An exhaustive view of a country's e-government initiatives can be seen from its survey result [20]. Finally, Kamaruddin and Noor [10] have proposed a "citizen-centric demand model for transformational government" which represents four components, namely Transparency, Participation, Openness and Responsiveness, as the essence of the model. Our research adopted this model as the components in classifying the characteristics of citizen-centric e-government websites as it is the most relevant to the context of this research. By doing so, the gaps left by the study will be fulfilled, as proposed by the authors [10].

3 Methods and Findings

The study was qualitative in nature and has utilized a triangulation of data collection methods by conducting literature analysis and performing websites' observation. The methods were chosen to provide a more holistic and better understanding of the phenomenon under study. Data collected were analyzed using thematic analysis, and the result yielded themes, components and characteristics of citizen-centricity. The characteristics were then validated against high-ranking e-government national portals, and the list of validated characteristics was used to develop the evaluation tool. To demonstrate its usage, the tool was deployed to a case study of Malaysia e-government websites.

3.1 Literature Analysis

Literature analysis consists of data collection and data analysis phases, and it was conducted to identify the characteristics of citizen-centric e-government websites. In doing data collection activity, literatures from various online databases within the research area have been explored and collected using keywords such as "citizen-centric government", "user-centric government", "citizen-oriented government", "user-oriented government", "open government", "transparent government", "responsive government" and "participatory government". According to Oxford-Dictionaries.com [21], "characteristic" is defined as, "a feature or quality belonging typically to a person, place, or thing which serves to identify them". Based on this definition, citizen-centric characteristics in the literatures were scrutinized and coded based on model proposed by Kamaruddin and Noor [10]. Table 1 listed four components of the model and its description. A list of citizen-centric characteristics was then categorized according to these components.

A total of 57 characteristics were gathered from the literatures and divided into the four components, where each component has between 6 to 31 characteristics depending on its related literatures. For instance, Transparency component contains six characteristics synthesized from five main literatures. The characteristics are social media; operation and activities information; sharing decision made; simple and understandable information; traceable process flow; and searching [10, 22–25].

The data analysis phase began when all characteristics were read carefully and repeatedly to understand its meaning and context of use. Thematic analysis method which emphasizes "pinpointing, examining, and recording patterns or themes within data" was used [26]. In this method, terms that have similar meaning were combined in groups and a word or phrase that best describes the characteristics from respective group was selected as a parent theme. The themes selections were generated using an inductive approach where the identified themes are "strongly linked to the data without trying to fit them into a pre-existing model or frame" [27]. Eight themes were generated during this process and used as parent themes for all the characteristics. The themes were named as Channel/Platform, Facility, Information, Quality, Usability, Application, Engagement Program and Communication. To illustrate the process, characteristics of Transparency component mentioned previously were now linked under its parent's theme, as shown in Table 2.

Table 1 Components of citizen-centric [10]

Component	Description
Openness	"Government provides free access to its structured and unstructured data"
Transparency	"Government provides information about their operations and decisions to the public"
Participation	"Citizens contribute to government's planning and decision-making and use government's data to create better service for the community"
Responsiveness	"Government listens to citizens' feedback and acknowledges it"

Table 2 Characteristic categorization for transparency component

No	Authors	Characteristic	Theme
1	[22, 23, 25]	Social media	Channel/Platform
2	[10]	Operation and activities information	Information
3		Sharing decision made	Information
4		Simple and understandable information	Information
5		Traceable process flow	Application
6	[24]	Searching	Information

Table 3 Description of characteristics in transparency component

No	Theme	Characteristic	Authors	Description
1	Channel / Platform	Social media	[22, 23, 25]	Promoting transparency, satisfaction and perceptions of public sector trustworthiness through social media
2	Information	Operation and activities information	[10]	Provide information about government operations and activities
		Sharing decision made	[10]	Provide information about government decisions
		Simple and understandable information	[10]	Provide simple to understand, relevant and honest information for the public to know
		Searching	[24]	Access points available for searching
3	Application	Traceable process flow	[10]	Clear and traceable process flow

To complete the structure, description for each characteristic was formulated and it was derived from literature analysis process that has been carried out before. Example of characteristics' description for Transparency component is depicted in Table 3.

3.2 *Websites Validation*

Citizen-centric characteristics that were analyzed in the literature analysis phase need to be validated to ensure they are a correct depiction of real world from the perspective of the intended use. According to 2016's Waseda report, "national portal is the foundation of e-Government and a basic interface for stakeholders to access government in an electronic way" [19]. For the validation process, an observation technique was performed, and the observation unit being used was e-government national portal. Selection of the national portals was based on their existence in both UN-EGDI and Waseda rankings, which means that the first five portals that appeared in both rankings have been selected to be observed. The national portals that fulfilled this criterion were UK, Australia, Korea, Singapore and New Zealand.

The characteristics of citizen-centricity were used as variables in the validation process. Each variable was coded with a binary value of "Yes" or "No" to denote the state of conformance toward the observation unit, starting from Openness and followed by Transparency, Participation and Responsiveness components. Using the characteristics descriptions, the selected e-government national portals were observed page by page to look for the features that conform to the characteristics that have been identified.

Each of the characteristics that conformed to the portals' features was given a "Y" (Yes) value, and those that did not conformed was given an "N" (No) value. "NA" (Not Applicable) value was recorded if the features could not be accessed or irrelevant to the context of the portals. Then, each characteristic was calculated and given a binary number based on majority count of the Y's and N's. The binary number one (1) represented conformance on the characteristics while zero (0) was a non-conformance. The method was in accordance with the commonly known democratic principle identified as "majority rule" [28]. Table 4 showed the observation findings in national portals that were linked to the Transparency component's characteristics.

Table 4 Observation result for characteristics in transparency component

No	Characteristic	E-government national portals					Value
		UK	AU	KR	SG	NZ	
1	Social media	Y	Y	Y	Y	Y	1
2	Operation and activities information	Y	Y	Y	Y	Y	1
	Sharing decision made	Y	Y	Y	Y	Y	1
	Simple and understandable information	Y	Y	Y	Y	Y	1
	Searching	Y	Y	Y	Y	Y	1
3	Traceable process flow	NA	NA	NA	NA	NA	NA

Table 5 Citizen-centric characteristics' conformance

No	Component	No. of characteristics	Conformance		
			Y	N	NA
1	Openness	31	21	4	6
2	Transparency	6	5	0	1
3	Participation	13	9	3	1
4	Responsiveness	7	4	2	1
Total		57	39	9	9

Results from Table 5 showed that most Transparency characteristics have returned a conformity value (1). However, “Traceable process flow” characteristic has returned a “NA” value to denote that this characteristic could not be validated using the observation technique. Overall, the result showed that majority of the Transparency characteristics that were derived from literatures conformed to the features adopted in selected e-government national portals during the validation process. The process is repeated with other components where, finally, total values were tallied, and validity of the characteristic was established. Table 5 showed result of conformance for all citizen-centric characteristics categorized by components.

It can be concluded that out of 57 characteristics of citizen-centric e-government websites identified from the literature analysis, nine characteristics were rejected in the website validation phase. Due to the research limitation, there were nine characteristics having returned the “NA” value. These characteristics could not be included in the final list of citizen-centric characteristics because its conformity was unknown, and thus, it will be researched further in future works. Finally, 39 characteristics have been identified as valid based on its conformance.

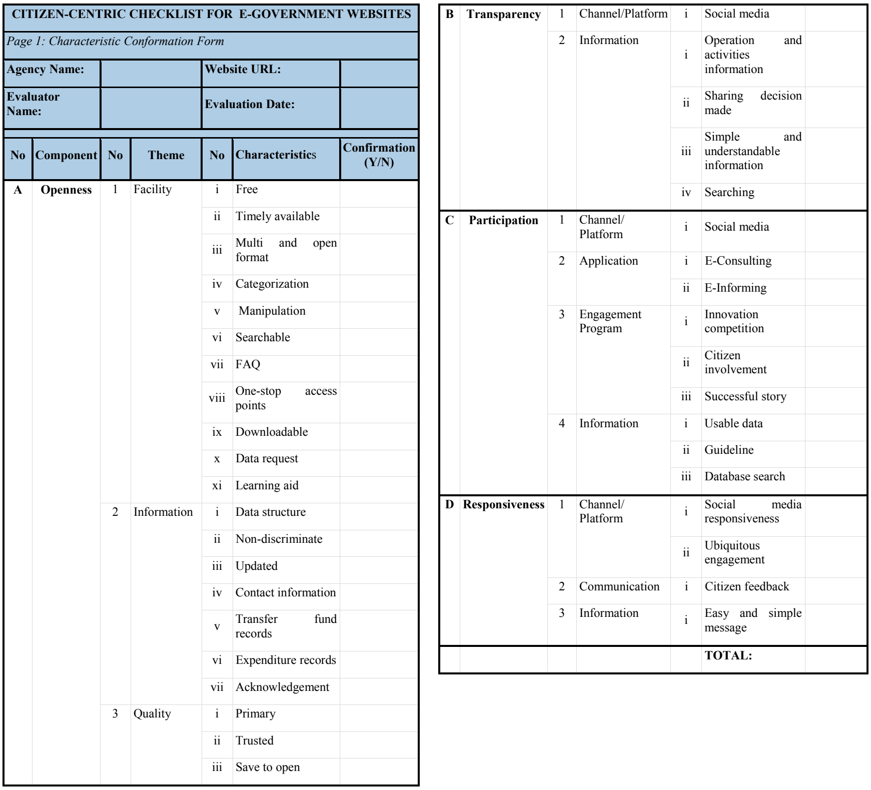
3.3 Evaluation Tool Development

All components, themes and characteristics were arranged to make up the checklist that will be used in the citizen-centric evaluation tool. The tool was named “Citizen-centric Checklist for E-government Websites” (CCEW) for easy reference and identification. In the header section of CCEW, fields of agency name, website URL, evaluator name and evaluation date were added to identify each evaluation activity. Figure 1 showed the first page of the CCEW which tabulated all the information that have been arranged into characteristics confirmation form. The form includes 39 characteristics that will be used as conformance variables for website evaluation.

To facilitate the website evaluation process, evaluators were also provided with a description of each component and characteristic in the second page of CCEW. Additional information concerning the theme description underlying each characteristic was also provided in the third page of CCEW. However, due to pages’ limitation, the second and third pages of CCEW are not included in this paper but available upon request from the author.

4 Application of Citizen-Centric Checklist for E-government Websites (CCEW)

The citizen-centric checklist for e-government websites was designed to be a guideline for evaluators of e-government websites from government or external agencies



CITIZEN-CENTRIC CHECKLIST FOR E-GOVERNMENT WEBSITES			
Page 1: Characteristic Conformation Form			
Agency Name:		**Website URL:**	
Evaluator Name:		**Evaluation Date:**	

No	Component	No	Theme	No	Characteristics	Confirmation (Y/N)
A	**Openness**	1	Facility	i	Free	
				ii	Timely available	
				iii	Multi and open format	
				iv	Categorization	
				v	Manipulation	
				vi	Searchable	
				vii	FAQ	
				viii	One-stop access points	
				ix	Downloadable	
				x	Data request	
				xi	Learning aid	
		2	Information	i	Data structure	
				ii	Non-discriminate	
				iii	Updated	
				iv	Contact information	
				v	Transfer fund records	
				vi	Expenditure records	
				vii	Acknowledgement	
		3	Quality	i	Primary	
				ii	Trusted	
				iii	Save to open	
B	**Transparency**	1	Channel/Platform	i	Social media	
		2	Information	i	Operation and activities information	
				ii	Sharing decision made	
				iii	Simple and understandable information	
				iv	Searching	
C	**Participation**	1	Channel/ Platform	i	Social media	
		2	Application	i	E-Consulting	
				ii	E-Informing	
		3	Engagement Program	i	Innovation competition	
				ii	Citizen involvement	
				iii	Successful story	
		4	Information	i	Usable data	
				ii	Guideline	
				iii	Database search	
D	**Responsiveness**	1	Channel/ Platform	i	Social media responsiveness	
				ii	Ubiquitous engagement	
		2	Communication	i	Citizen feedback	
		3	Information	i	Easy and simple message	
					TOTAL:	

Fig. 1 Page 1 of Citizen-centric checklist for E-government websites: characteristic confirmation form

mandated to perform e-government websites evaluation. Prior to performing the evaluation, evaluators need to understand each of the characteristics by reading through the characteristics and themes description provided with the evaluation tool. After that, the evaluations may take place by identifying of website to be evaluated and making sure that it is accessible during the evaluation period. Some information regarding the evaluation activity such as the agency's name who owned the websites, websites' URL, evaluator's name, and evaluation date need to be filled out prior to the evaluation session for the purpose of reference and record-keeping. During the evaluation activity, conformance on any characteristics can be marked using Y, N or NA value. Y value refers to the characteristic's compliance while N value refers to its non-compliance. NA value can be given when the characteristic being assessed is not related to the nature of the organization's process.

At the end of the evaluation activity, number of characteristics that are in conformance will be calculated and given a total percentage. Attention should also be given to the characteristics with N value. Websites' owners should be made aware of the result while taking necessary actions to comply with the non-conformance characteristics. This should be done to show significance of the evaluation, indicate agency's readiness for the next evaluation cycle and most importantly to meet the needs of the citizens.

4.1 Case Study: Malaysia E-government Websites Evaluation

Malaysia Digital Economy Corporation (MDEC) is the government agency who was overseeing e-government websites evaluation in Malaysia. In 2005, MDEC has introduced an independent mechanism to evaluate the government agencies' websites named Provider-Based Evaluation (ProBE), or previously known as Malaysia Government Portals and Websites Assessment (MPGWA), with the objective to establish standardization of Malaysia e-government websites. ProBE was intended to increase the quality of information and services via 7 Pillars of User Expectations, complementing the Malaysia User Satisfaction Evaluation (MUSE). With the development of CCEW, the tool will be deployed in Malaysia's e-government context to gauge the level of citizen-centricity in its e-government websites. Thirty e-government websites that have scored 5-stars rating, which is the highest score in ProBE's 2016 report, were selected as the subject of evaluation.

Result of Websites Evaluation

Table 6 showed the analysis of website evaluation result for thirty government agencies' websites in Malaysia. The citizen-centric conformance score column showed the total marks attained by each agency's websites divided over the total score. Some websites were evaluated against 39 characteristics, while some had only 38 applicable characteristics to be evaluated with. For instance, the characteristic of "funds transfer data" in Openness component was not counted because it was not relevant to websites being assessed. The score for each citizen-centric component and total percentage were then calculated, tabulated and ranked as below.

Using this tool, evaluators can rank e-government websites under scrutiny based on the total percentage score. Evaluators can also identify which contents or features that are lacking based on each citizen-centric component's score, after which adaptive maintenance can be done by the website owners. The findings of the evaluation can reveal which portals or websites that showed good conformance to the citizen-centric approach in its design and delivery of e-services.

Table 6 Website evaluation result analysis

Rank	Agency Name	Website URL	Citizen-centric conformance score	Citizen-centric component score				Total score (%)
				Openness	Transparency	Participation	Responsiveness	
1	Department of Chemistry Malaysia	http://www.kimia.gov.my/	38/38	20/20	5/5	8/8	4/4	100
2	Majlis Agama Islam dan Adat Istiadat Melayu Kelantan	http://www.e-maik.my	37/39	21/21	5/5	7/9	4/4	94.9
3	Companies Commission of Malaysia	http://www.ssm.com.my/	36/38	19/20	5/5	8/9	4/4	94.7
3	Labuan Corporation	http://www.pl.gov.my	36/38	19/20	5/5	8/9	4/4	94.7
3	Lembaga Kemajuan Bintulu	http://www.bda.gov.my	36/38	19/20	5/5	8/9	4/4	94.7
3	Ministry of Urban Wellbeing, Housing and Local Government	http://www.kpkt.gov.my	36/38	20/20	4/5	8/9	4/4	94.7
3	Accountant General's Department of Malaysia	http://www.anm.gov.my/	36/38	20/20	5/5	8/9	3/4	94.7
3	Department of Statistics, Malaysia	https://www.dosm.gov.my/	36/38	20/20	5/5	8/9	3/4	94.7
4	Department of Environment	http://www.doe.gov.my	35/38	19/20	5/5	8/9	3/4	92.1
4	Kuala Langat District Council	http://www.mdkl.gov.my/	35/38	18/20	5/5	8/9	4/4	92.1

(continued)

Table 6 (continued)

Rank	Agency Name	Website URL	Citizen-centric conformance score	Citizen-centric component score				Total score (%)
				Openness	Transparency	Participation	Responsiveness	
4	Malaysia Productivity Corporation (MPC)	http://www.mpc.gov.my	35/38	19/20	5/5	7/9	4/4	92.1
4	Minerals and Geoscience Dept Malaysia	http://www.jmg.gov.my	35/38	19/20	5/5	7/9	4/4	92.1
4	Ministry of Home Affairs	http://www.moha.gov.my/	35/38	20/20	5/5	7/9	3/4	92.1
4	Penang State Government	http://www.penang.gov.my	35/38	20/20	5/5	7/9	3/4	92.1
5	Port Dickson Municipal Council	http://www.mppd.gov.my	34/38	17/20	5/5	8/9	4/4	89.5
5	Judicial and Legal Training Institute	http://www.ilkap.gov.my/	34/38	18/20	5/5	7/9	4/4	89.5
5	Office of The Johor State Secretary	http://www.johor.gov.my/	34/38	19/20	5/5	6/9	4/4	89.5
5	Melaka State Government	http://www.melaka.gov.my	34/38	18/20	5/5	8/9	3/4	89.5
6	Jabatan Agama Islam Sarawak	http://www.jais.sarawak.gov.my	34/39	18/21	5/5	7/9	4/4	87.2
7	Department of Veterinary Services	http://www.dvs.gov.my/	33/38	18/20	4/5	7/9	4/4	86.8

(continued)

Table 6 (continued)

Rank	Agency Name	Website URL	Citizen-centric conformance score	Citizen-centric component score				Total score (%)
				Openness	Transparency	Participation	Responsiveness	
7	Perak Land and Mines Office	http://ptg.perak.gov.my/	33/38	19/20	4/5	7/9	3/4	86.8
7	Seremban Municipal Council	http://www.mpsns.gov.my	33/38	18/20	5/5	7/9	3/4	86.8
7	Perak State Government	http://www.perak.gov.my/	33/38	18/20	5/5	7/9	3/4	86.8
7	Parliament of Malaysia	http://www.parlimen.gov.my/	33/38	19/20	5/5	6/9	3/4	86.8
7	Public Services Commission of Malaysia	http://www.spa.gov.my/	33/38	17/20	5/5	7/9	4/4	86.8
8	Pentabiran Bahagian Mukah	http://www.mukah.sarawak.gov.my/	32/38	17/20	5/5	7/9	3/4	84.2
9	Pentabiran Bahagian Betong	http://www.betong.sarawak.gov.my/	31/38	18/20	4/5	6/9	3/4	81.6
10	Yayasan Islam Kelantan	http://www.yik.edu.my/	31/39	16/21	5/5	7/9	3/4	79.5
11	Kementerian Utiliti Sarawak	http://mou.sarawak.gov.my/	30/38	18/20	4/5	5/9	3/4	78.9
12	Malaysian Meteorological Department	http://www.met.gov.my/	27/38	14/20	4/5	5/9	4/4	71

5 Conclusion

The research adds to the field of e-government by developing an evaluation tool for measuring citizen-centricity in government online services and demonstrating application of the tool in Malaysia's e-government websites. The Citizen-centric Checklist for E-government Websites can help to identify what is lacking in e-government websites design and delivery by providing a content checklist of important characteristics that should be present in e-government websites. It was designed to be a guideline for evaluators of e-government websites from government or external agencies assigned to perform e-government websites evaluation. Future research can be done to enhance CCEW by including weightage for each of its components and characteristics to make the score more accurate.

Refining e-government websites to meet citizen-centric e-government requirements will have a major impact on how services will be delivered, which will eventually encourage higher level of take-ups of government online services. Nevertheless, it could also improve public service delivery because successful services are built on an understanding of what the citizens need. Thus, it is believed that the findings in this study will be helpful to the government to prioritize and focus on their websites quality aspects that put citizens' satisfaction as the top priority.

Acknowledgements The authors would like to thank the Research Management Centre (RMC), Universiti Teknologi MARA (UiTM), Shah Alam for the financial support from FRGS-RACER Research Grant (600-IRMI/FRGS-RACER 5/3 (085/2019)).

References

1. Sigwejo A, Pather S (2016) A citizen-centric framework for assessing E-government effectiveness. Electron J Inf Syst Dev Countries 74(1):1–27
2. Lemke F, Taveter K, Erlenheim R, Pappel I, Draheim D, Janssen M (2019) Stage models for moving from E-government to smart government. International conference on electronic governance and open society: challenges in Eurasia. Springer, Cham, pp 152–164
3. Kamau G, Njihia J, Wausi A (2016) E-government Websites User Experience from Public Value Perspective: Case Study of Itax Website in Kenya. In: 2016 IST-Africa week conference, IEEE, pp 1–8
4. Saha P (2010) Enterprise architecture as platform for connected government: understanding the impact of enterprise architecture on connected government. National University of Singapore Institute of Systems Science
5. Luna-Reyes LF, Gil-Garcia JR, Celorio Mansi JA (2011) Citizen-centric approaches to Egovernment and the back-office transformation. In: Proceedings of the 12th annual international digital government research conference on digital government innovation in challenging times—Dg.o '11, 213
6. Verkijika SF, De Wet L (2018) A usability assessment of E-government websites in sub-Saharan Africa. Int J Inf Manage 39:20–29
7. Singh H, Kar AK, Ilavarasan PV (2017) Assessment of E-governance projects: an integrated framework and its validation. In: Proceedings of the special collection on eGovernment innovations in India, pp 124–133

8. Osman IH, Anouze AL, Irani Z, Al-Ayoubi B, Lee H, Balcı A, Medeni TD, Weerakkody V (2014) COBRA framework to evaluate E-government services: a citizen-centric perspective. Gov Inf Q 31(2):243–256
9. Wang L (2010) Evaluating government web site with a citizen-centric approach. Syracuse University
10. Kamaruddin KA, Noor NL (2017) Citizen-centric demand model for transformational government systems. In: Proceedings of twenty first Pacific Asia conference on information systems. Langkawi
11. Rahim MM, Alharbi I (2014) User satisfaction with E-government websites: an australian experience. In: Proceedings of 17th international conference on computer and information technology (ICCIT), IEEE, Dhaka, pp 245–249
12. Gupta DN (2008) Citizen-centric approach for e-governance. In: Argawal A, Ramana VV (eds) Foundations of e-governance: proceedings of the 5th international conference on e-governance, Hyderabad, India, pp 39–54
13. Misra DC (2006) Defining E-government: a citizen-centric criteria-based approach. In: 10th national conference on e-Governance, pp 1–11
14. Zibret B, Derca M, Miklic N (2009) How to become a citizen-centric government. Report of AT Kearney Inc. Retrieved October, 30, p 2014
15. Wang L, Bretschneider S, Gant J (2005) Evaluating web-based E-government services with a citizen-centric approach. In: Proceedings of the 38th Hawaii international conference on system sciences, Hawaii
16. Zahran DI, Al-nuaim HA, Rutter MJ (2015) A critical analysis of E-government evaluation models at national and local municipal levels. Electron J E-Gov 13(1):28–42
17. Eschenfelder KR, Miller CA (2007) Examining the role of web site information in facilitating different citizen-government relationships: a case study of state chronic wasting disease web sites. Gov Inf Q 24(1):64–88
18. United Nations (2016) United Nations e-Government Survey 2016 e-Government in Support of Sustainable Development [online]. Retrieved from http://www.un.org/desa
19. Obi T (2016) The 12th Waseda–IAC international e-Government rankings survey 2016 report, Waseda University Institute of e-Government. Retrieved online from http://www.teg.org.tw/common/dl.jsp
20. Malaysia Government Portal & Website Assessment (2013) Retrieved from http://www.mscmalaysia.my/sites/default/files/mgpwa/MGPWA2013.pdf
21. Characteristic (n.d) In OxfordDictionaries.com. Retrieved June 18, 2017, from https://en.oxforddictionaries.com
22. Al-Aufi AS, Al-Harthi I, AlHinai Y, Al-Salti Z, Al-Badi A (2017) Citizens' perceptions of government's participatory use of social media. Transforming Gov: People Process Policy 11(2):174–194
23. Porumbescu GA (2016) Linking public sector social media and E-government website use to trust in government. Gov Inf Q 33:291–304
24. Thornton JB, Thornton E (2013) Assessing state government financial transparency websites. Ref Serv Rev 366–387
25. Bertot JC, Jaeger PT, Grimes JM (2012) Promoting transparency and accountability through ICTs, social media, and collaborative e-government. Transforming Gov: People Process Policy 6(1):78–91
26. Braun V, Clarke V (2006) Using thematic analysis in psychology. Qual Res Psychol 3(2):77–101
27. Boyatzis RE (1998) Transforming qualitative information: thematic analysis and code development. SAGE, Thousand Oaks, CA
28. Eraslan H, Merlo A (2002) Majority rule in a stochastic model of bargaining. J Econ Theory 103(1):31–48

An Application Framework for Blockchain on Smart Factory Locations Using a Datacenter Approach

Awatef Salem Balobaid, Saahira Ahamed, Shermin Shamsudheen, Padmanayaki Selvarajan, Praveetha Gobinathan, and Betty Elezebeth Samuel

Abstract We offer an in-pocket platform which allows data providers, virtual servers and AI designers to collaborate for machine knowledge representations in a permission less AI marketplace. The information is a valuable numerical tool that is important for group's perspectives. Our initiative assists data owners in protecting data access and security while supporting AI developers' use of their data for training. Comparably, AI developers can use the calculation tools from the cloud provider against relinquishing power or privacy. Our framework protocols are designed to allow all three entities data owners, cloud vendors and AI developers to legitimately increase their behavior in the public system to test and approve of misconduct or conflict arbitration with the blockchain system. The Hyperledger Fabric is an analogy to centralized AI networks that do not have protection for information prior to modeling. We present investigational outcomes which show dormancy in various access networks where blockchain colleagues are accessible via dissimilar data centers. Our findings specify that the planned approach is well tailored to numerous data. Also, model owners can educate up to 70 models to a 12-peer un-optimized blockchain system and some 30 prototypes to a 24-peer framework.

A. S. Balobaid (✉) · S. Ahamed · S. Shamsudheen · P. Gobinathan · B. E. Samuel
Department of Computer Science, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia
e-mail: asbalobaid@jazanu.edu.sa

S. Ahamed
e-mail: sahamed@jazanu.edu.sa

S. Shamsudheen
e-mail: sdheen@jazanu.edu.sa

P. Gobinathan
e-mail: pthan@jazanu.edu.sa

B. E. Samuel
e-mail: bsameul@jazanu.edu.sa

P. Selvarajan
Department of Information Technology and Security, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia
e-mail: psilvaraan@jazanu.edu.sa

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_33

Keywords Blockchain · Data owners · Data centers · Cloud vendors · AI · Privacy · Frameworks

1 Introduction

Some AI markets [1–6] are being built by various people in the AI Value Chain as a shared platform for linking, generating and monetizing AI properties, such as data and models. They also encourage innovation, the wise use of AI and equal value distribution through the development and use of AI resources. Take, for example, a group of k-hospitals who have healthcare information but lack collective expertise in designing AI models. In the meantime, computer scientists in research and business typically lack access to clinical health information.

In this sense, the IT market should provide a way to safely construct models for assessing the health of the patients between hospitals (i.e., data owners) and IT developers. In addition, GPU computing resources can be provided to train these models, and other developers can use the building blocks of any model. Finally, businesses, including clinical companies, insurance companies and pharmaceutical companies, will explore and ingest these models. The fact that they don't protect data and models [7–9] is a crucial impediment to the growth of both regulated and decentralized AI economies. As a result, model owners will quickly drop control of their properties and therefore they cannot sustainably get value from them. Due to both the legal limitations [10] and because owners may sacrifice strategic IP and economic gain, large-scale data sharing or models might not be practical. In addition, centralized AI markets rely on a trustworthy central authority to retain a verifiable data-sharing and training audit trails that can establish digital dominations, raise costs, and become vulnerable to manipulation.

In this research, a blockchain-based approach is built using architecture that maintains anonymity and ownership protection of AI properties in a non-trusted, central IP sector. We have three courses in our framework: consumer behavior, model makers (MOs) and cloud owners (COs) which allow them to practice AI models together with open datasets [11] constitute federalized learning. In our organization, data protection is assured by devising each dataset into many COs such that no single organization has access to the full datasets on the blockchain. To construct the model, each CO with its data subset will take part in different training sessions, using federalized learning. Model anonymity is assured by completely homomorphic coding training models, making model forecasts unreliable without the coding [12].

Our framework was developed via the Hyperledger Fabric open source [13], in which all stakeholders communicate with the system via chain code functions (e.g., consistently smart agreements on Ethereum system). We present the design of these purposes, which promote the true documenting of all blockchain transactions, including splitting and dissemination of datasets and the preparation and implementation of several training courses among COs. This guarantees that the framework offers verifiable proof of anticipated actions or misconduct and the settlement of conflicts while strengthening trust with stakeholders.

For instance, the system helps an MO to confirm that the information DO provides is the data sufficient to train the model. An MO also should ensure that a new design focused on its transfer learning has already been created, rather than provide a copy of a classification network from each CO engaged in confederal training. Our approach has been deployed in blockchain sites with up to 24 independent entities, each containing three separate pairs. The duration and effective conduct of these communications in different network settings is demonstrated by activities pertaining to the mutual training of predictive analytics and studies. Our experiments have already shown that our method is well-balanced and can be used for 75 prototypes per second with related latencies in data gathering in block chain.

2 Related Works

The privacy of information sharing environments also models exercise where information, models and computing tools provided in an untrustworthy environment involves effective protocols and channels to document and validate the action process by multiple stakeholders in the correct manner. These stakeholders include owners of data (DO), owners of clouds (CO) and models (MO). The DO's provide broad proprietary datasets (e.g., customers) that are highly useful for reliable AI models to be educated by three industry stakeholders, namely health care, autonomous vehicles, and compliance information. Without losing control of this data, people often desire to monetize and sell it for AI training in safe, transparent and reliable ways.

DOs extend their reach and money gains, through community participation. COs are cloud providers that want to train AI models with servers and GPU computers. The COs broaden their user base to offer subscription and data storage services as part of the business at a reasonable cost. MOs are AI designers with the ability and experience to build advanced AI models, but who lack the appropriate data for the training of frameworks.

MOs want to make money with their trained models and do not want to risk control of their representations during the course of their training. As part of a business, MOs can grant admission to various information structures, compute resources from COs at reasonable costs, effectively minimize the total cost of AI training models and satisfy their training requirements. The MOs can also use their datasets. Figure 1 illustrates the numerous industry actors who are inspired by their personal economic profits to compete in the market. The protocol starts with ex-DOs wanting to exchange their data in the AI training marketplace.

Any connection to the entire data collection will, however, lead to data leakage from those in the system. The DOs will theoretically exchange encrypted datasets to protect their integrity, so AI training on encrypted data needs to be conducted. But if trained models are wanted by MOs, the inferencing of models will again entail the flow of data in an encoded form. This suggests that MOs will essentially rely on

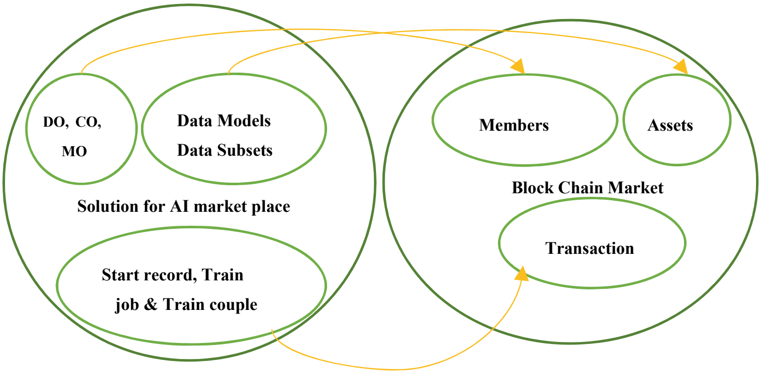


Fig. 1 Blockchain system [14]

DOs for the encoding of new input information for prediction deduction or future decryption.

After datasets are circulated to COs, they are available for business AI training. These data subsets are referred to as data security subsets (PPDS). An MO uses data samples to construct a model and gets approval to train the model on the whole dataset. An MO creates a model, and since the information set is spread through different COs, our framework uses federated education to train the AI models in which every CO receives training in the process. However, in joined learning, all COs have admission to the last classical model which means that during the training process, MOs are losing their control of their models.

To avoid this, the MOs decrypt their models by means of spatial domain transcription. Each round is shared with all COs by the running variant of the authenticated model. The MO combines independently trained models to override the amendment to the bill with the CPs for a second round of testing. The final, training encrypted model is then obtained. Each CC uses its own information subset to train the encoded classical model. Because MOs access partly qualified models at the conclusion of each round, they can also learn more about the features of each CO's data. To sidestep this, an accidental array of COs with datasets may be used for preparation. In this way, the data feature of individual COs is unlikely to be decoded and thus the data keeping method maintains full integrity, provided that all data subsections are eventually included in several subsequent training rounds.

3 Proposed System

The separation and duplication of a dataset by DO between separate COs is one of the first steps involved in collective preparation. These two steps in our approach are taken intelligently to guarantee that the possession of the dataset is protected, and because uncooperative. COs often refuse to say that their models have been trained

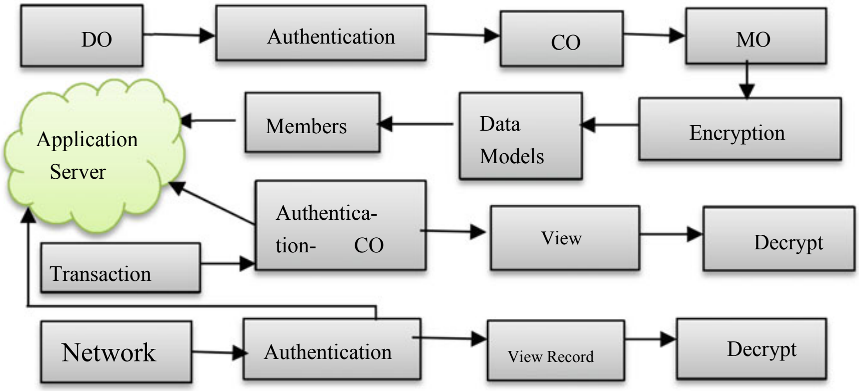


Fig. 2 Proposed workflow of the blockchain methodology

using their data subsets without training them. The DO concludes an off-chain deal with multiple COs and provides those data subsets safely, as previously stated. No data is recorded on the blockchain to ensure the anonymity in our approach regarding the real data collection (Fig. 2).

The DO breaks the dataset to ensure that the whole dataset is partially protected by every CO. In comparison, splitting is carried out in a distorted manner, i.e., no subsection has all data groups or values. Furthermore, no subset has most information from a single class. The primary requirement means that no single CO can extract useful knowledge around the dataset, while the additional safeguards require that our approach involves around 37 different transactions. These transactions use numerous queries or model implementations, equivalent to properties, for the cooperation of various stakeholders. Around 15 are specifically ordered from various participants, while the others are requested by other transactions. A few important transactions are listed below.

The StartRound transaction is used through MOs to trigger the exercise process by selecting a variety of accidental databases which are autonomously trained for federated learning by the cloud owner. The data attributes cannot be viewed by the MO. With regard to blockchain-recorded steps, the DO generates a CI example by using the 'CreateCI' contract for each chain of distributed data. 'Free' is the early condition, and all COs are told. The COs wait vigorously for blockchain proceedings and each CO will be able to obtain the data out of network from the DO upon the receipt of a notification. Each CO knows the identity of the DO, but none of the COs know one another (Fig. 3).

A fraudulent CO may say that a data subset different from that given by the DO is obtained. Our protocol allows the CO to announce the hash on the blockchain of the data subset to prevent this situation. The CO records in the asset CI the hash values of its data subset and uses the JoinCI transaction to change the blockchain hash value. The DO checks the haze proclaimed by the CO for its own computation of the dataset hash distributed to the CO by consulting the blockchain. If an error occurs, the DO

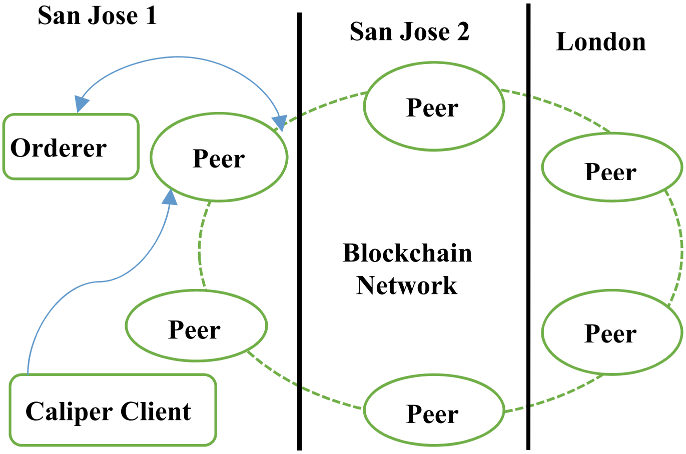


Fig. 3 Implementation of blockchain

will mark the CO as deceitful. The DO uses the transaction to 'verify' the position of the CI, if they see a similar hash, then it will not be checked.

This phase guarantees that the CO does not receive a faulty data subset. Data masses that are developed are prepared for training when a DO reviews the patch of a CO database subset and labels the managed CI status. A false CO may also assume that the model has learned on its subsection without the training required to save GPU's methodical cash. If the DO exchanges and analyzes the data and chunks that are held by different COs, it is able to guide the implementation system by the federation. The DO discloses facts about its dataset and a written arrangement to authorize an MO to study this expertise and to use the training dataset.

When an MO is confident of the dataset and of the contract, they want to train a model of the AI in their dataset. Model confederal learning is carried out in rounds. The MO supplies all COs with the latest running prototype at all training rounds, as the data collection is distributed over several COs. At the end of the exercise round, the MO will receive efficient copies of all COs and enforce them on a solitary cooperate model, usually by average. The MO agrees with end specifications for model evaluations, i.e., measures metrics for the federated model to decide if more model training is appropriate.

As for the recorded order of processes on blockchain, the representations are mainly specified as characteristics, an MO uses 'CreateMod' to develop a blockchain prototype object case. The model object includes: Owners ID Template, ID Template, Professional Model, URL Model, Hash Model and Training Process. The model type defines the type of AI classical (e.g., DT, neural network). After multiple exercise rounds, the model URL reveals the current model version. Each CO needs to conduct the training in the training process. The area of hash value contains the hash proclaimed after a workout by a CO.

This is used to verify the MO as it installs the qualified aggregation models. An MO communicates its intention to build and train a model using the smart contract 'OrderTC' to create a Train Couple (TC) entity in the blockchain. The dataset and the model object are described when the TC is generated. In the TC object, the 'status' area monitors the various training phases. Blockchain notifies the DO that a model owner wants to train on the dataset when a TC is generated. To approve the model training, the DO uses 'ApproveTC' transaction to set the 'APPROVED' status area. This helps DO to check that several demands have been received and model training accepted by the same MO. The same transaction used by the DO to authorize the TC to monitor the development of individual workers produces an asset called Train Job (TJ) or the training of each of the datasets.

Consequently, a corresponding TJ is available for any CI. The training continues with an MO calling on the intelligent contract transaction 'StartRound'(SR). The SR transaction enters the TC and specifies the dataset (and essentially the PPDS) used to train the model in this round. While federated learning facilitates education with all PPDSs owned by various COs, our approach uses a random collection of PPDSs for each training round. Both repeated units for the selected PPDS are taken into consideration. A random collection of PPDS in each training session guarantees that MOs cannot deduce any useful data on COs by means of the partly trained models collected during each training session. However, several rounds of training mean that entirely PPDS are used for exercise. At the end of SR, blockchain lifts the announcement to every CO picked for that round by PPDS and replicated units.

4 Results and Discussion

All 15 transactions have been introduced by us with chain code capability. These transactions allow all protocol operations and full model training exercises to be carried out. Two essential metrics have been evaluated: latency and the performance characteristic for distribution systems that require scalability. Our tests have been conducted with blockchain components approved by the Docker container server on Soft-Layer servers (Hyperledger fabric Version 1.2.0-rc1). A separate server of 32 core and 64 GB RAM, running Ubuntu16.04, was provided for each portion.

Caliper Hyperlinker is used as benchmarking tool (or Caliper). In a number of conventional use scenarios, Caliper lets users measure the efficiency of blockchain runs. It provides reports with a variety of metrics of efficiency, including tps, latency, etc. Both our experiments use the cloth as a standard default organization enters. This resembles the blockchain overall behavior, and better responses can be expected in simplified environments. The block dimensions were of 500 for all our tests, and the block duration was one. The standard training block policy has been taken into account as 2:3:1. Transaction demand amounts were 250tps, 520tps and 1080tps. We tried to raise the purchasing rates otherwise but measurements dropped drastically. For 1 million transfers, each study was performed tenfold. All runs were registered on average. Blockchain peers were set up to replicate tests closer to true situations

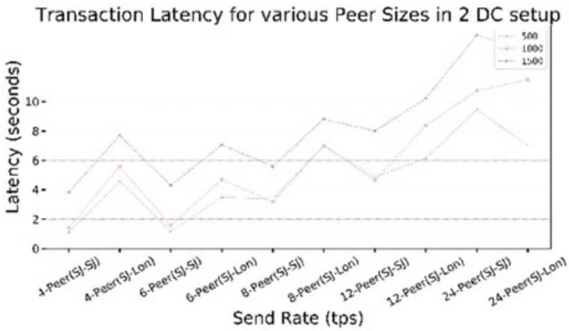


Fig. 4 Latency comparison

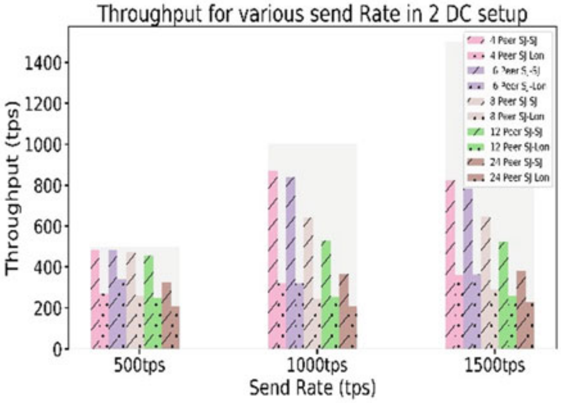


Fig. 5 Throughput comparison

in multiple locations faithfully. We considered up to 24 pairs anywhere and two DC areas, namely San Jose and London Node, were placed within an information center (single DC) or around information center locations that have been checked (2 DC setup). We had two settings in the 2 DC configuration. One of the geo-places was San Jose 1 in addition San Jose 2, while the other was between the geographies of San Jose 1 and London. The number of pairs was similarly divided between two pages. For example, in San Jose two pairs were in a 4-peer network, and two pairs were in London. Figure 4 displays the network structure in various areas used in our tests. In San Jose, we had one customer and one ordering node in same location (Fig. 5).

5 Conclusion

The availability of detail and data security, as well as the privacy paradigm that resulted in loss of value and ownership, hindered the development of centralized and decentralized AI markets. In a decentralized and trustworthy AI market, we proposed a new framework for preserving the privacy and possession of property through the blockchain. Our system chain code purposes were structured to motivate parties to log their behavior in the distributed chain such that there can be proof of their intended conduct, to prevent, misdeed and conflict settlement in the underlying blockchain system. Our Hyperledger Fabric deployment reveals that our framework promoted a robust model education and offered a realistic option for centralized AI programs that does not ensure information before model protection. It protects the secrecy of the distribution of records. The smart contract is activated when the requirements for accessing the record are met, and the comparing task is carried out accordingly. It is capable of ensuring the legitimacy and equity of data exchange.

References

1. Buterin V et al (2014) A next-generation smart contract and decentralized application platform. white paper 3:37
2. Clack CD, Bakshi VA, Braine L (2016) Smart contract templates: foundations, design landscape and research directions. arXi preprint arXiv:1608.00771
3. Savelyev A (2017) Contract law 2.0:'smart'contracts as the beginning of the end of classic contract law. Inf Commun Technol Law 26(2):116–134
4. Rota N, Thonnat M (2000) Activity sequences using declarative models. In: ECAI, pp 673–680. Citeseer
5. Samek W, Wiegand T, Müller K-R (2017) Explainable artificial intelligence: understanding, visualizing and interpreting deep learning models. arXiv preprint arXiv:1708.08296
6. Larimer D (2014) Delegated proof-of-stake (dpos). Bitshare whitepaper
7. Dorri A, Kanhere SS, Jurdak R, Praveen Gauravaram, Lsb (2017) Lightweight scalable blockchain for iot security and privacy. arXiv preprint arXiv:1712.02969
8. Gruber D, Li W, Karame G (2018) Unifying lightweight blockchain client implementations. In: Proc. NDSS Workshop Decentralized IoT Security Stand., pp 1–7
9. Schrijvers O, Bonneau J, Boneh D, Roughgarden T (1089) Incentive compatibility of bitcoin mining pool reward functions. In: International Conference on Financial Cryptography and Data Security, pages 477–498. Springer, 2016.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science
10. Lewenberg Y, Bachrach Y, Sompolinsky Y, Zohar A, Rosenschein JS (2015) Bitcoin mining pools: a cooperative game theoretic analysis. In: Proceedings of the 2015 international conference on autonomous agents and multiagent systems, pp 919–927. Citeseer
11. Khatoon S, Javaid N (2019) Blockchain based decentralized scalable identity and access management system for internet of things
12. Poon J, Dryja T (2016) The bitcoin lightning network: Scalable off-chain instant payments
13. Eberhardt J, Tai S (2017) On or off the blockchain insights on off-chaining computation and data. In: European conference on service oriented and cloud computing, pp 3–15. Springer
14. Baranwal Somy N et al (2019) Ownership preserving AI market places using blockchain. In: 2019 IEEE international conference on blockchain (Blockchain), pp 156–165 IEEE, Atlanta, GA, USA. https://doi.org/10.1109/Blockchain.2019.00029

Comparison of the Improved Control of Three-Phase Two-Level and Multi-level Inverters with Sinusoidal (SPWM) and Space Vector (SVPWM) Control for Grid-Connected Photovoltaic Systems (PV)

Abdelhak Lamreoua, Anas Benslimane, Jamal Bouchnaif, and Mostafa El Ouariachi

Abstract This article is a proposal toward improved control of the three-phase two-level and multi-level photovoltaic inverter with two new control methods, by the sinusoidal (SPWM) and space vector (SVPWM) control for a nonlinear load. The contribution of this study concerns the strategies of control of the active and reactive power injected by this inverter in the grid in order to improve the losses of harmonics current in the grid. The main objective of this method is to respond to the problems encountered with the photovoltaic inverter to effectively filter the harmonics of the current. After comparing the results of the two systems, our findings suggest that the current THDi of the interlaced (multi-level) inverter is lower than that obtained with the two-level inverter, provide higher-quality waveforms, reducing current and losses caused by high-frequency harmonics. The simulation results demonstrate the effectiveness of these propose techniques in this work.

Keywords Three-phase photovoltaic inverter · Sinusoidal (SPWM) · Space vector (SVPWM) · Multi-level inverter · Total harmonic distortion (THD)

1 Introduction

Currently, harmonic distortion sources have become an increasingly serious concern as more PV is integrated into the grid system [1, 2] and can represent a high total harmonic ratio in small systems [3, 4]. Unfortunately, there are several disadvantages inherent to conventional inverter [5, 6], including a better efficiency and higher cost [7, 8], as well as the use of complex control method [9, 10]. The proposed

A. Lamreoua (✉) · J. Bouchnaif · M. E. Ouariachi
Laboratory of Electrical Engineering and Maintenance (LEEM), BP: 473 Higher School of Technology, University of Mohammed I, Oujda, Morocco

A. Benslimane · M. E. Ouariachi
Laboratory Renewable Energy, Embedded System and Information Processing, National School of Applied Sciences, University of Mohammed I, Oujda, Morocco

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_34

control commonly used with the photovoltaic inverter-based Space Vector Pulse Width Modulation (SVPWM) [11], and sinusoidal Pulse Width Modulation (SPWM) control [12–14], to limit the effect of an inherent third harmonic injection and correct the unbalanced system [15, 16]. The contribution of this paper concerns the strategies of control of the active and reactive power injected by this inverter in the grid [17–19]. The main objective of this method is to respond to the problems encountered with the photovoltaic inverter to effectively filtered the harmonics of the current. This article that is presented here is about the simulation and modeling of a system *PV* connected to the power grid using a two-level inverter and interlaced multi-level inverter with four cells in parallel [20, 21], in order to optimize the losses in the semiconductors as well as the improvement of yield and financial cost [22, 23]. The work presented here is about the modeling and the command improvement of the multi-level inverter detailed in Sect. 1. The results obtained and the comparison of the order of the two and multilevel structures are presented in the Sect. 2.

2 Three-Phase Two-Level Inverter and Three-Phase Multi-level Inverter Modeling

2.1 Three-Phase Two-Level Photovoltaic Inverter Modeling

The three-phase structure of Fig. 1 shows three connection functions (h1, h2 and h3), three-phase-source voltages (v10, v20 and v30), three-phase voltages (v1N, v2N and v3N) and a qualified voltage v0N zero sequence voltage such as:

$$v_{k0} = h_k * \frac{U}{2} \tag{1}$$

$$v_{k0} = \frac{1}{3}\begin{vmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{vmatrix}\begin{vmatrix} h1 \\ h2 \\ h3 \end{vmatrix} * \frac{U}{2} \tag{2}$$

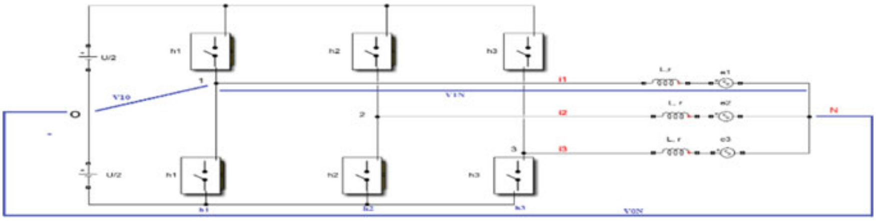


Fig. 1 Block structure of the three-phase PV inverter

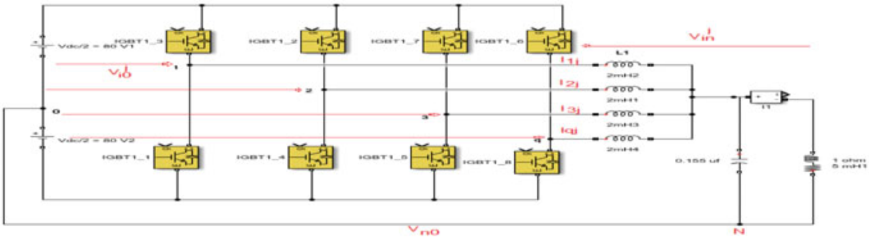


Fig. 2 Simplified block of the interlaced inverter (for one phase)

2.2 Three-Phase Multi-level Inverter Modeling

Photovoltaic system connected to the grid using an interlaced inverter (q = 4). The control is obtained by comparing a modulating sine-wave ($Vj*$; $j = 1,2,3$) of frequency $f = 50$ Hz with q high frequency triangular carrier waves ($fsw = 20$ kHz. The architecture of our system is composed of a PV generator which is replaced by a voltage source Vdc, an interlaced inverter, a LC filter, and the grid. Each phase of the inverter is made up of $q = 4$ arms. From Fig. 2, we will note that the quantities, $Vi0j$ is the voltage of cells, $Vinj$ is the voltage on the inverter side, $Vj2$ is the voltage of the grid, and Vj3 is the vector current in the cells of switching of the inverter.

2.3 The Command Strategy

The PQ command strategy applied to the inverter is presented in Fig. 3. The strategy of control and identification of harmonics is done in our case by the instantaneous

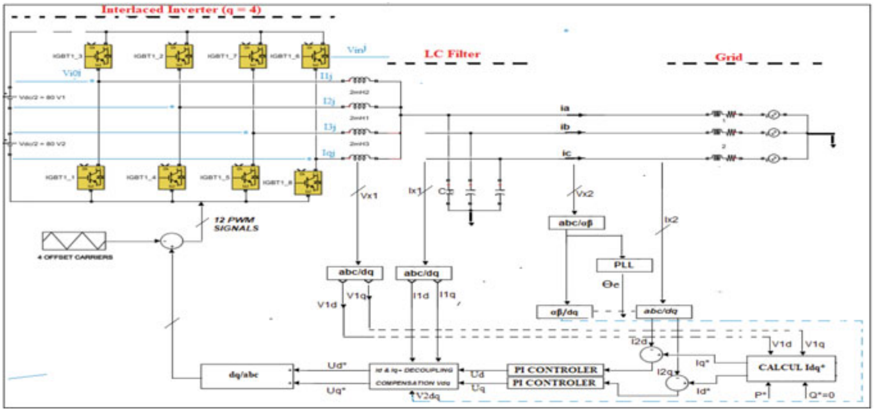


Fig. 3 General structure of the command strategy

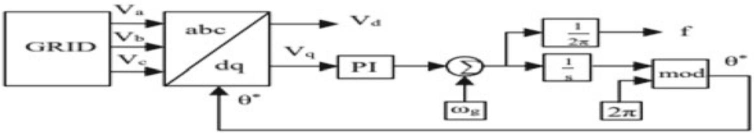


Fig. 4 Block diagram of the PLL algorithm

power p q method, with two control loops, one to control the current and the other to control the voltage. The Matrix [L] transforms the three-phase currents into $dq0$ system as shown in (Eq. 3)

$$\begin{bmatrix} i_d \\ i_q \\ i_0 \end{bmatrix} = [L]\begin{bmatrix} i_A \\ i_B \\ i_C \end{bmatrix} \text{with } [L] = \sqrt{\frac{2}{3}}\begin{bmatrix} \sin\alpha & \sin\left(\alpha - \frac{2\pi}{3}\right) & \sin\left(\alpha + \frac{2\pi}{3}\right) \\ \cos\alpha & \cos\left(\alpha - \frac{2\pi}{3}\right) & \sin\left(\alpha + \frac{2\pi}{3}\right) \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{3}$$

The transfer function in the system dq is given by Eq. (4):

$$G_{PI}^{(dq)}(s) = \begin{bmatrix} K_p + \frac{K_i}{s} & 0 \\ 0 & K_p + \frac{K_i}{s} \end{bmatrix} \tag{4}$$

Phase Locked Loop Algorithm.

The estimated angle ($\theta*$) of the voltage is fed back to operate the *abc* to *dq* block so that the Park rotation can be performed [12].

Control parameters.

See Table 1.

3 Simulation Results

3.1 Three-Phase Two-Level PV Inverter

Output current–voltage waveforms by sinusoidal control (SPWM):

Before filtering. Figure 5a shows the harmonic spectra, without the harmonic compensation loop. The system current and voltage harmonic distortion rate is: total harmonic distortion of current and voltage equal to 4.40% and 4.47%, respectively, with an output current rich in harmonics and are very far from the fundamental, which causes quality problems of current injected, due to the connection to the nonlinear load.

After filtering. A system waveform using a harmonic compensation is shown in Fig. 5b. The output harmonics and unbalanced current of phase in the PV inverter are compensated, after using filtering on the system. Figure 5b shows that the proposed

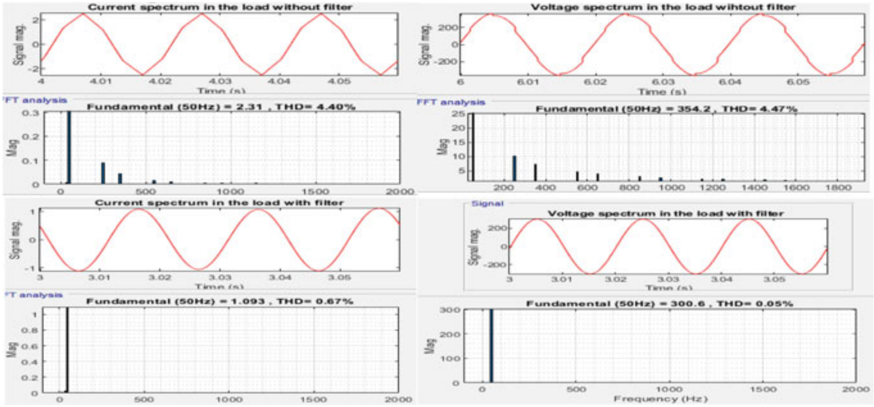


Fig. 5 Grid current and voltage FFT spectrum **a** before filtering and **b** after filtering

control can reduce the THD in the system from to THDi = 4.40% and THDv = 4.47% to THDi = 0.68% and THDv = 0.05% respectively ≪3% (international standard).

Output current and voltage waveforms by Space Vector control (SVPWM):

Before filtering. When the load is connected to the grid, the total harmonic distortion in the system before compensation is THDi = 4.39% and THDv = 4.47%. Figure 6a shows that the fundamentals obtained follow the reference, with harmonics of frequencies close to carrier and of large amplitude, which guarantees easy fundamental filtering.

After filtering. Figure 6b shows that the output current quality for PV inverter is improved after using the proposed harmonic compensator loop.

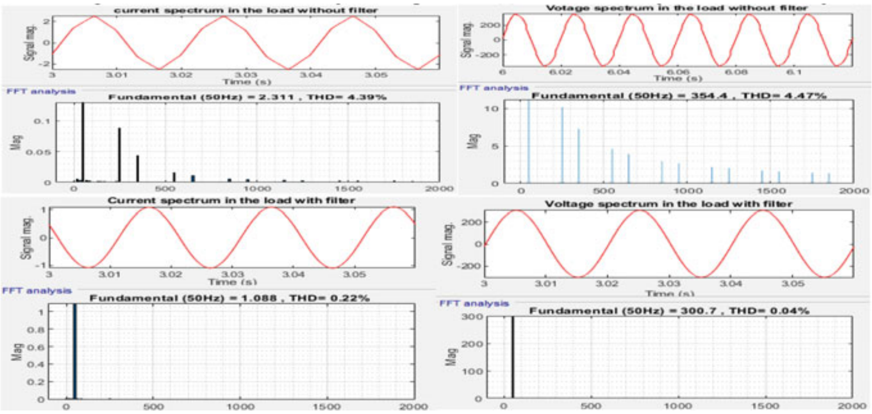


Fig. 6 Grid current and voltage FFT spectrum **a** without filtering, **b** filtering

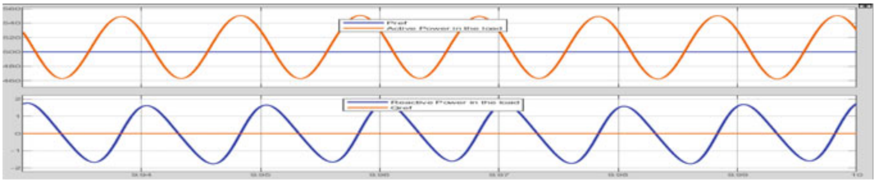


Fig. 7 P and Q waveforms in the load after compensation

The effects of the used control strategy which can be observed by the THD value of the system are lower than that obtained with regulation before filtering; the THDi of current and voltage equal successively 0.22% and 0.04% ≪3%.

Average value of the P and Q at the output of the inverter.

From Fig. 7, we notice that the power P equal their reference value (P = Pref) and the power (Q = Qref = 0) close to the zero value (or very small value).

3.2 Three-Phase Multi-level Inverter (Interlaced Inverter q = 4)

Before the filtering of frequency harmonics in Fig. 8a, the one-shaped output signals are not purely sinusoidal because of the harmonics of currents and voltage. After applying filtering, the current and voltage curves in Fig. 8b, the waveforms are almost sinusoidal and identical. This shows the strength of the interlaced inverter and the quality of its waveform. We also note the improvement in the transient state of the curves obtained with the interlaced inverter system compared to the transient regime

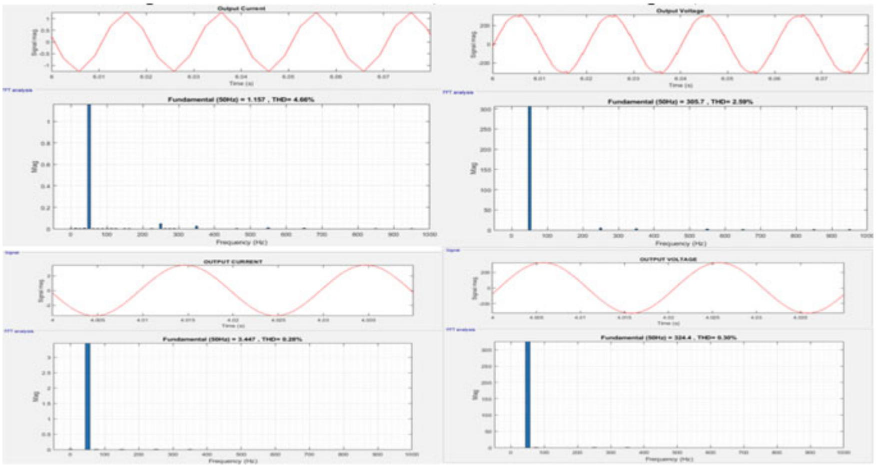


Fig. 8 Grid current and voltage FFT spectrums; **a** before filtering and **b** after filtering

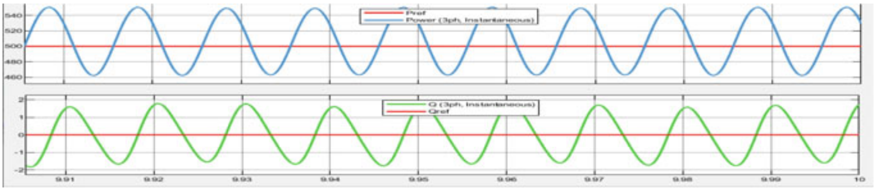


Fig. 9 P and Q power waveforms after compensation

with conventional inverter. The total harmonic distortion of current and voltage is respectively **THDi = 0.28%** and **THDv = 0.30%** for the 50 first harmonics, unlike the indicators of *THD* obtained by the system before filtering (**4.66%** and **2.59%**), the indicators *THD* of the system using an interlace inverter after filtering are much better. This shows that the *THD* indicators of the system using an interlaced inverter are much better than that obtained with the conventional inverter. We also note that the improvement in the transient regime of the curves obtained with the interwoven inverter system after filtering compared to the transient regime of the curves of the system with a conventional inverter.

Average value of the P and Q at the output of the inverter.

The average value of the P and Q power at the output of the multi-level inverter typology after application of the proposed control as seen in Fig. 9.The Qr value is set to zero (Qr = Qref = 0), while the Pa has a value of the reference (Pa = Pref).

Comparison of total harmonic distortion of these two typologies is explained in Table 2. So by comparing the values from the spectral analysis, it could be seen that the total THD of the multi-level three-phase photovoltaic inverter topology equal to THDi = 0.28%(SPWM)- THDi = 0.23% (SVPWM) and THDv = 0.30% is lower than in the two-level three-phase photovoltaic inverter typologies. Also, the *PLL* succeeded in synchronizing both conventional and interlace inverter system. Thus, we were able to observe a clear improvement in the transient regime and the waveforms for of the interlaced inverter system compared to the two-level system. It is the same for the total harmonic distortion (*THD*). The *THD* of current and voltage is respectively 0.28% (SPWM)-0.23% (SVPWM) and 0.30% in the case of the system with interlaced inverter against 0.67% (SPWM)-0.22% (SVPWM) and 0.05 for the classic system.

Table 1 Design parameters

Photovoltaic power	500 W
V_{dcref}	80 V
I_{min}	1A
Fg	50 Hz
f_{pwm}	10 kHz

Table 2 Comparison of total harmonic distortion of these two typologies

	Topology	control	THD Current (%)	THD Voltage (%)
Before filtering	Three-phase two-level inverter	SPWM-SVPWM	4.40–4.39	4.47–4.47
After filtering			0.67–0.22	0.05–0.04
Before filtering	Three-phase multi-level inverter	SPWM-SVPWM	4.66–4.66	2.59–2.59
After filtering			0.28–0.23	0.30–0.30

4 Conclusion

This article is a contribution toward the improvement of the control of the three-phase two-level and multi-level photovoltaic inverter, with a new control strategy, by the sinusoidal (SPWM) and space vector (SVPWM) control for a nonlinear load.

The comparison of the results of the two systems shows that the current THDi of the interlaced (multi-levels) inverter is lower than that obtained with the two-level inverter, provide higher-quality waveforms, reducing current and losses caused by high-frequency harmonics. We notice too that the performance of the multi-level three-phase photovoltaic inverters is better than that obtained with the two-level three-phase photovoltaic inverter. We observed a clear improvement in the transient regime and the waveforms in the two cases. Moreover, the current THDi of the interlaced inverter is lower than that obtained with the two-level inverter. From the simulation results, we can demonstrate the efficiency of the multi-level three-phase photovoltaic inverters. The *THD*i of current are respectively 0.28% (SPWM) and 0.23% (SVPWM) in the case of the system with interlaced inverter against 0.67% (SPWM) and 0.22% (SVPWM) for the two-level photovoltaic inverter and obtain a high-quality grid (THDi% < 5%). We conclude that this method responds, in terms of cost and energy efficiency, to the problems encountered with the photovoltaic inverter, and effectively compensates the harmonics current injected in the grid. In order to justify the suitability of the proposed inverter control, we started to validate the simulations performed via an experimental setup in the next step.

References

1. Lamreoua A, Benslimane A, Messaoudi A, Aziz A, El Ouariachi M (2018) Comparison of the different commands direct and indirect of a single-phase in-verter for Photovoltaic'. In: ICEERE international conference on electronic engineering and renewable energy, Laboratory of Electrical Engineering and Maintenance (LEEM), BP:473 Higher School of Technology, University of Mohammed I, Oujda, Morocco, April (2018), pp 576–586
2. Wei J, Bai D, Yang L (2015) Polymer photovoltaic cells with rhenium oxide as anode interlayer. PLoS One 10:e0133725. https://doi.org/10.1371/journal.pone.0133725 PMID: 26226439 2 (Public Library of Science)
3. Trinh Q-N, Lee H-H (2014) An enhanced grid current compensator for grid-connected distributed generation under nonlinear loads and grid voltage distortions. IEEE

4. Timbus A, Liserre M, Teodorescu R, Rodriguez P, Blaabjerg F (2009) Evaluation of current controllers for distributed power generation systems. Power Electron IEEE Trans IEEE 24:654–664
5. Xu G, Moulema P, Ge L, Song H, Yu W (2016) A unified framework for secured energy resource management in smart grid. Smart Grid 73–96 (CRC Press)
6. Golovanov N, Lazaroiu GC, Roscia M, Zaninelli D (2013) Power quality assessment in small scale renewable energy sources supplying distribution systems. Energies 6:634–645 (Multidisciplinary Digital Publishing Institute)
7. Sultani JF (2013) Modelling, design and implementation of D-Q in single-phase grid connected inverters for photovoltaic systems used in domestic dwellings. Faculty of Technology De Montfort University Leicester, UK
8. Noman AM, Addoweesh KE, Alabduljabbar AA, Alolah AI (2019) Cascaded H-bridge MLI and three-phase cascaded VSI topologies for grid-connected photovoltaic systems with distributed MPPT. Int J Photoenergy 2019. Article ID 7642919, 22 pages. https://doi.org/10.1155/2019/7642919
9. Naderipour A, Guerrero JM (2017) An improved synchronous reference frame cur-rent control strategy for a photovoltaic grid-connected inverter under unbalanced and nonlinear load conditions. PLOS ONE. 10.1371 journal pone 0164856 Feb 13, 2017
10. Bengourina MR (2017) Direct power control of a grid connected photovoltaic system, associated with an active power filter. Revue des Energies Renouvelables 20(1):99–109
11. Lamreoua A, Benslimane A, Bouchnaif J, El Ouariachi M (2021) An improved sinusoidal (PWM) and vector (SVPWM) current control for a three-phase photovoltaic inverter connected to a non-linear load. In: Proceedings of ICEERE 2020. https://doi.org/10.1007/978-981-15-6259-4_51.Print ISBN: 978-981-15-6258-7. Online ISBN: 978-981-15-6259-4n
12. RaoVadlamudi SV (2016) Decoupled DQ-PLL with Positive Sequence Voltage Normali-zation for Wind Turbine LVRT Control; 25–27 Oct 2016, Sands Expo and Convention Centre, Marina Bay Sands, Singapore
13. Bengourina MR (2017) Direct power control of a grid connected photovoltaic system,associated with an active power filter. Revue des Energies Renouvelables 20:99–109
14. Purushotham M (2019) Reinforced droop for active current sharing in parallel NPC inverter for Islanded AC microgrid application. MDPI energies, 11 Aug 2019
15. Mahamat C, Petit M, Costa F (2018) Analyse et commandes des convertisseurs multi-niveaux pour un générateur photovoltaïque connecté au réseau électrique. Energie électrique. Université Paris Saclay (COmUE), 2018. Français. ffNNT: 2018SACLN024
16. Wu T-F, Chang C-H, Lin L-C, Yu G-R, Chang Y-R (2014) A D-Σ digital control for three-phase inverter to achieve active and reactive power injection. IEEE Trans Industr Electron 61(8):3879–3890
17. Naderipour A, Guerrero JM (2017) An improved synchronous reference frame current control strategy for a photovoltaic grid-connected inverter under unbalanced and nonlinear load conditions. PLOS ONE. 10.1371 journal pone 0164856 February 13, 2017
18. Jain P, Deshmukh SP (2020) Design of three-phase five-level cascaded H bridge inverter with boost converter. Int J Electron Pages 478–498
19. RaoVadlamudi SV (2016) Decoupled DQ-PLL with positive sequence voltage normali-zation for wind turbine LVRT control. Sands Expo and Convention Centre, Marina Bay Sands, Singapore 25–27 Oct 2016
20. Purushotham M (2019) Reinforced droop for active current sharing in parallel NPC inverter for Islanded AC microgrid application. MDPI energies 11 Aug 201
21. Hasan MM, Abu-Siada A, Islam MR (2016) Design and implementation of a novel three-phase cascaded half-bridge inverter. IET Power Electron. ISSN 1755-4535
22. S. M. I. M. M. L.-C. L. a. C.-W. H. Wu TF (2017) An improved resonant frequency based systematic LCL filter design method for grid-connected inverter. IEEE Trans Ind Electron. https://doi.org/10.1109/TIE.2017.2682004

23. Babaei E, Alilu S, Laali S (2014) A new general topology for cascaded multilevel inverters with reduced number of components based on developed H-bridge. IEEE Trans Ind Electron 61(8):3932–3939
24. Houssem Chaouali HO (2017) Improving the control strategy of a standalone photovoltaic pumping system by fuzzy logic technique. (IJACSA) Int J Adv Comput Sci Appl 8(3)

Senior Citizens' Training Experience in Secure Electronic Payment Methods

Clara Lucía Burbano González, Miguel Ángel castillo Leiva, Alex Torres, and Sandra Rodriguez Álvarez

Abstract Virtual training is a mechanism that enables contemporary society to be literate, allowing up-to-date information on the technological environment, improving cognitive abilities as well as soft skills required in the workplace where individuals can develop their maximum performance. The following article presents results obtained in the literacy of older adults of Santiago de Chile, belonging to the Los Andes Compensation Fund in the area of Information Security in Electronic Payment Means, through the application of the alternative action research method under an apprehensive level methodology of the comparative analytical type of quantitative data, oriented in the development of a virtual object that allows to reduce the knowledge gap and lose the fear of the use of technology through the integration of media literacy and informational (MIL) focused on the transmission of updated knowledge and training in technological resources.

Keywords Learning and knowledge technologies (TAC) · Media and information literacy (AMI) · Computer security · Andragogy · Electronic payment methods

1 Introduction

Technology has transformed our environment from face-to-face to virtuality, inverting the interaction with individuals, allowing active communication between the community through technology, due to the massive sending of information

C. L. B. González (✉) · M. Á. Leiva
Mayor University, Santiago, Chile
e-mail: clara.burbano@umayor.cl

M. Á. Leiva
e-mail: miguel.castillo@mayor.cl

A. Torres · S. R. Álvarez
University Corporation Comfacauca-Unicomfacauca, Popayán, Colombia
e-mail: atorres@unicomfacauca.edu.co

S. R. Álvarez
e-mail: srodriguez@unicomfacauca.edu.co

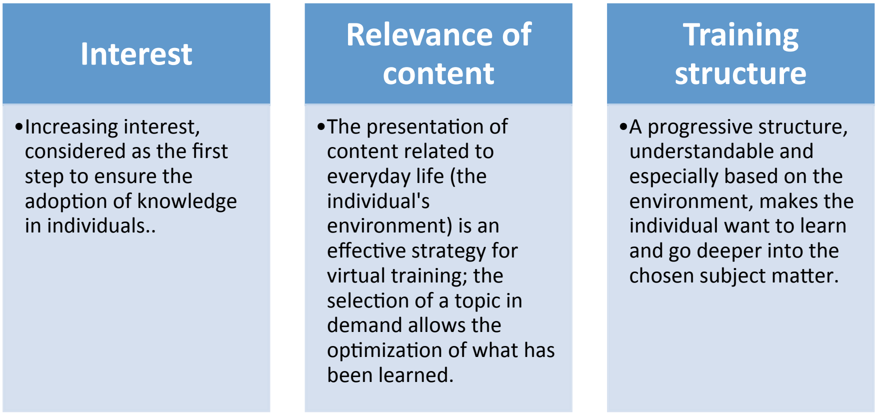
X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_35

considered a slow, imprecise and above all complex process. However, with the technological evolution, the speed at which information is accessed has increased, increasing accuracy as an essential characteristic, which encompasses resources such as databases, microprocessors and servers, to provide immediate response to user requests. Decreasing the complexity of technology allows it to be accessible to all types of people in society to be appropriated effectively [1]. The above perspective evidences the need to train society in technological aspects related to the use of secure tools, allowing end users to access with peace of mind [2]; in this sense, efforts to transform learning have migrated toward the search for tools that contribute to improve knowledge, keeping it accessible and available to the whole society. In this sense, it was proposed from the Magister in Cybersecurity of the Universidad Mayor de Chile, the use of a technological tool in which andragogy (training of the elderly) is applied from the appropriation of technology (virtual learning object (OVA)) based on media and information literacy (AMI) as a structure to finally bring knowledge to older adults enrolled in the Caja de Compensación los Andes-Chile in the safe use of electronic means of payment; through the development of the article, it will be possible to observe the results obtained in the experience of training older adults in electronic means of payment and the process carried out to reach an appropriate solution in the intervention of society and especially to train in impact topics according to the technological evolution of the twenty-first century defined as the networked society [3].

2 Methodology of Experience

The development of the training experience of the older adult is a process where understandable and extensive contents are integrated; permeating the knowledge in such a way that it is transformed from a block of information to a component that can be molded to the experience and use of the knowledge by the individual. An older adult does not learn at the same pace as a child, young person or adult; in the first instance, it must be guaranteed to capture the interest, breaking the barrier and allowing the training experience to be enjoyable; secondly, relevant content must be captured where the older adult has in practice related to the environment, so that processes, use and appropriation of information can be simplified; thirdly, the training structure from the perspective of meaningful learning promotes the decentralization of knowledge by uniting the aforementioned aspects in a final product for a defined period of time for a selected population, and, finally, it generates an "update" of knowledge from experience and work [4]. The above can be seen in the following Fig. 1.

The development of the training experience of the older adult is a process where understandable and extensive contents are integrated; permeating the knowledge in such a way that it is transformed from a block of information to a component that can be molded to the experience and use of the knowledge by the individual.



Interest

- Increasing interest, considered as the first step to ensure the adoption of knowledge in individuals..

Relevance of content

- The presentation of content related to everyday life (the individual's environment) is an effective strategy for virtual training; the selection of a topic in demand allows the optimization of what has been learned.

Training structure

- A progressive structure, understandable and especially based on the environment, makes the individual want to learn and go deeper into the chosen subject matter.

Fig. 1 Interest, relevance and structure for virtual training in older adults

In order to reach this result, a literature review was carried out with the following conceptual categories: (a) Use of TAC in media and information literacy (AMI), strategy for the transmission of knowledge and the formation of skills and needs of contemporary individuals; (b) technological mediations from virtual learning objects (VLO), a tool to convert face-to-face learning focused only on content, a decentralized strategy where the teacher ceases to play the role of connoisseur/trainer and becomes a companion/mediator, giving his previous role to the learner so that he can make his own decisions about the learning modality to which he best adapts; (c) cybersecurity in secure electronic means of payment, represents the specific knowledge, relates strategies to make secure payments and reduces the technological gap, transforms the resilience to change that sustains the study population (older adults recognized by the Caja de Compensación Los Andes-Chile), evolution and adoption of knowledge through digital channels, promoting cyberculture as well as training in older adults.

2.1 Learning and Knowledge Technologies (LKT) in Media and Information Literacy (MLI)

Education is a right for everyone, regardless of race, sex or even age, where the latter aspect has revolutionized the way we think when building a technological tool that contributes to the acquisition of knowledge in any area. In the case of older adults, it is important to highlight that they do not have the same capabilities as children or young people, who will be alert to any change in their learning environment; on the contrary, older adults will only accept learning if it is something they do on a daily basis and in a repetitive manner, classifying new information into three types: "It is useful for my life"; "Maybe I will use it later"; "It is definitely not useful for me."

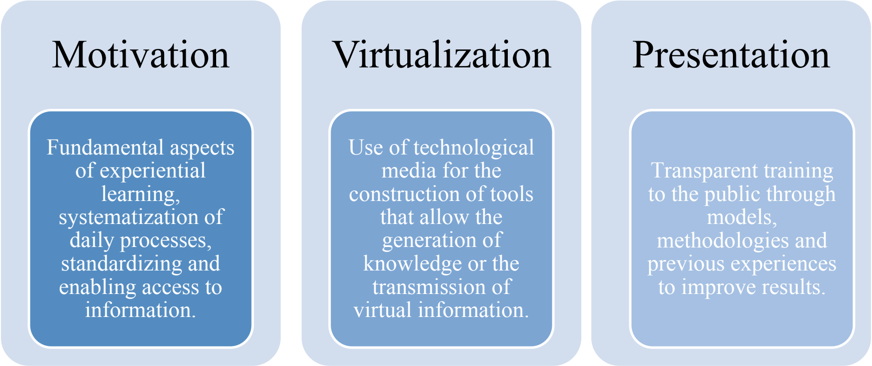

Motivation
Fundamental aspects of experiential learning, systematization of daily processes, standardizing and enabling access to information.
Virtualization
Use of technological media for the construction of tools that allow the generation of knowledge or the transmission of virtual information.
Presentation
Transparent training to the public through models, methodologies and previous experiences to improve results.

Fig. 2 Triangulation of knowledge toward the formation and transmission of knowledge in the older adult

They are linked to the needs of those who really need the knowledge, therefore, at all stages of cognitive development, for the development of technology in society.

Figure 2 contemplates three fundamental pillars that allow to generate in the individual/learner, an optimal experience from a virtual learning object (VLO); however, there is still a doubt about what is a VLO; in this sense and in a simplified way. it can be segmented into two parts: "Virtual object" and "learning." A "virtual object" is a set of digital resources that can be reusable and easily accessible in order to ensure that the individual develops skills and competencies visually, at their own pace and didactically; the "learning" is focused on the acquisition of knowledge through a medium where study, exercise and experience are used to learn. From the above, it is possible to observe the instrument (virtual object) and the technique (learning) which leads to identify that a virtual learning object is the composition between the instrument and the technique to be dynamic and interactive toward the acquisition of knowledge mediated by technological tools [5].

3 Methodological Design

The study was carried out by means of the degree thesis entitled "Training of the elderly in secure electronic means of payment," focused on the projective research methodology, consisted in finding the solution to practical problems and was concerned with establishing how to work to achieve ends and function adequately [6]. It proposed the elaboration of a model to solve the related problem/need. The action research method of quantitative type, made it possible to analyze data from a population of 40 seniors recognized in the compensation fund of Chile, taking a sample of 12 individuals, a pre- and post-test was conducted to know the level of adoption of knowledge about electronic means of payment before and after implementing the process by the OVA SIMPA-APP, conformed by the quantitative research approach.

4 Results

4.1 Cronbach's Alpha Consistency Test and Intervention Results

Determining the method of internal consistency by finding Cronbach's Alpha allows determining the reliability of a measurement instrument, reliability assessment becomes an indispensable process used in the measurement of attributes of interest; the reliability of a test to determine the state of knowledge before and after interaction with the OVA SIMPA-APP, allowed studying the properties of measurement scales; the reliability analysis procedure. The above scale measures a highly correlated characteristic [7]; the closer the value of Cronbach's Alpha test is to one (1), the higher the internal consistency of items analyzed for measuring the state of knowledge in secure electronic means of payment in older adults. The result can be seen below when calculating Cronbach's Alpha coefficient to determine the state of knowledge of secure electronic means of payment in older adults:

Table 1 determines the result obtained in the application of Cronbach's Alpha; the reliability of the test in each of its applications presents a good level of confidence (Cronbach's Alpha > 0.8) in the Likert measurement scale. Selecting a focal group of twelve older adults as the unit of analysis with estimated ages between 45 and 58 years, residents in the city of Santiago de Chile-Chile (analysis variable), a test was structured and developed with two intervention times: (a) Pre-test (before); (b) Post-test (after), applied to the aforementioned group, with the following two intervention times: (a) Pre-test (before); (b) post-test (after). (a) Pre-test (before); (b) post-test (after), applied to the aforementioned group. In this sense, by means of Table 1, the results were consolidated according to the scores obtained by each older adult, presenting the variation percentage value, which described the relationship between the pre-test and post-test values. The transformation and impact of the technological mediation contributed to achieve an optimal development of knowledge with a 218.1% improvement; in principle, it is consolidated that the strategy fulfilled its established purpose in training older adults from an OVA on the electronic means of payment in a safe way. Figure 3 shows the results obtained from the calculation of the mean in relation to the pre/post-test interventions, where a positive impact of technological mediation on knowledge formation can be seen:

Table 1 Reliability coefficient calculation result

Tool	Cronbach's alpha	Decision
Pre-test	0.81	Good
Post-test	0.96	Excellent

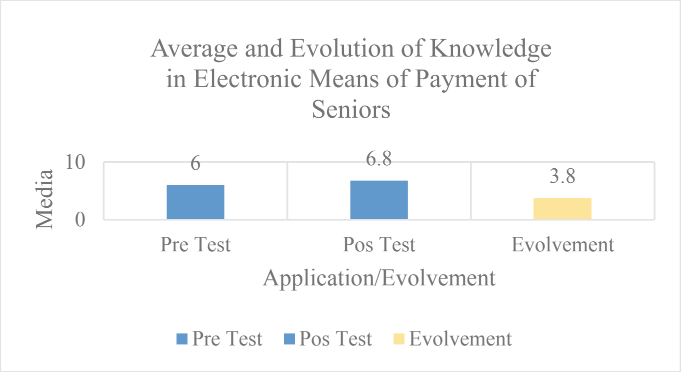


Fig. 3 Average and evolution of knowledge in electronic means of payment of older adults

4.2 Pedagogical Usability

The information society poses an ecosystem where ICT play a leading role in the economy, politics and especially education [8]. This implies the use of various technopedagogical mechanisms aimed at the design of educational materials using digital formats as modeling applications [9]. Characteristics of pedagogical usability evaluated by experts in pedagogy, ICT in education and computer security to ensure that both the content and platform used are effective and obtain the greatest possible impact on older adults; in this sense, the evaluation of usability has 15 questions which were rated on a Likert scale set from 1 to 5, where 1 is the lowest score and 5 was established as a minimum viable point, obtaining the following results (Fig. 4):

The figure above determines the final percentage obtained by the heuristic evaluation of 86% of compliance with the requirements established in the evaluation of experts; the conclusion is that the SIMPA-APP Tool is interactive, understandable,

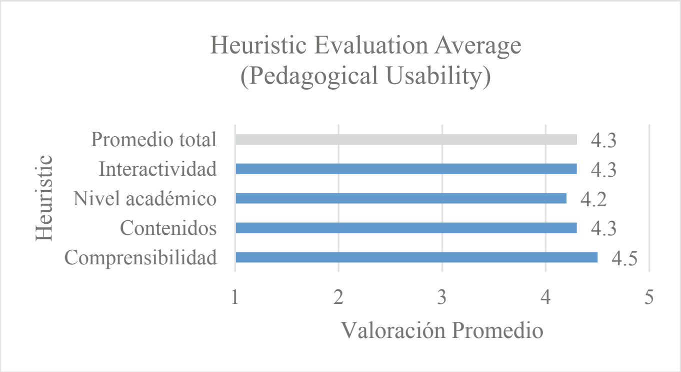


Fig. 4 Average of heuristic evaluation (pedagogical usability)

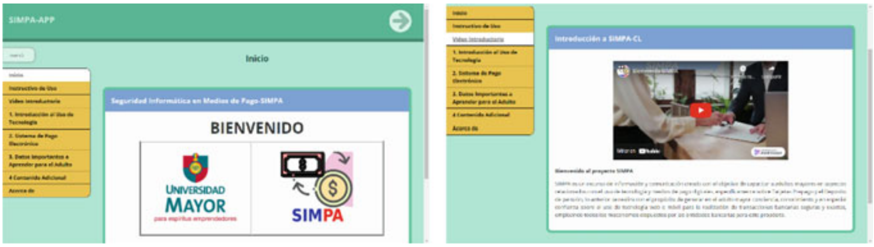

SIMPA-APP
Inicio
Inicio
Instructivo de Uso
Video Introductorio
1. Introducción al Uso de Tecnología
2. Sistema de Pago Electrónico
3. Datos Importantes a Aprender para el Adulto
4 Contenido Adicional
Acerca de
Seguridad Informática en Medios de Pago-SIMPA
BIENVENIDO
UNIVERSIDAD MAYOR
para espíritus emprendedores
SIMPA
Introducción a SIMPA-CL
Bienvenido al proyecto SIMPA

Fig. 5 SIMPA-APP OVA screenshots

of impact and with a good academic level to carry out the training process of older adults in the specific knowledge of secure electronic means of payment. Below are some screenshots of the SIMPA-APP Virtual Learning Object (VLO) (Fig. 5):

5 Conclusion

The Experience of Training Older Adults in Secure Electronic Means of Payment shows that technology is taking a leading role in the transmission of knowledge, especially by integrating knowledge nomads (Knowmads) in learning and self-training processes mediated by Information and Communication Technologies (ICT) [10]; this study identifies, analyzes, designs, develops and implements an impact training strategy under the guidelines of andragogy, allowing the training of older adults in secure payment methods for the use of technology in everyday life, making them understand the operation, uses and applications of new trends.

The results obtained in the development of the research show that older adults had an improvement in the appropriation of knowledge in secure electronic means of payment. In the words of the individuals: "This training strategy is an opportunity to acquire new knowledge on topics that are found in the environment every day; therefore, I feel fortunate to be part of the society of change," perception of those who opt for resilience in the use of technology and appropriation of new knowledge in constant evolution and construction of an ideal world.

References

1. López Bonilla LM, López Bonilla JM (2011) Models of adopting information technologies from the attitudinal paradigm. Cad. EBAPE.BR 9(1):176–196. https://doi.org/10.1590/S1679-39512011000100011
2. Azofeifa Bolaños JB (2017) Evolución conceptual e importancia de la andragogía para la optimización del alcance de los programas y proyectos académicos universitarios de desarrollo rural. Rev. Electrónica Educ. (Educare Electron. Journal) 21(1):1–16. https://doi.org/10.15359/ree.21-1.23

3. Castells M (1996) La sociedad red. [Online]. http://s3de4d611b4ec3006.jimcontent.com/download/version/1393284927/module/9140750878/name/La_sociedad_red_capitulo_2._Castell_Manuel.pdf
4. Mogollón E (2012) Una perspectiva integral del adulto mayor en el contexto de la educación. Rev Interam Educ Adultos 34:74 [Online]. https://www.redalyc.org/pdf/4575/457545090005.pdf
5. Morales Martín LY, Mendoza Nieves LG, Ariza LM (2016) Guía para el diseño de objetos virtuales de aprendizaje (OVA). Aplicación al proceso enseñanza-aprendizaje del área bajo la curva de cálculo integral. Rev Científica Gen. José María Córdova 14(18):127–147. [Online]. http://www.scielo.org.co/pdf/recig/v14n18/v14n18a08.pdf
6. Córdoba MN, Monsalve C (2008) Tipos de investigación, predictiva, interactiva, confirmatoria y evaluativa. Fund. Sypal, pp 139–140 [Online]. http://2633518-0.web-hosting.es/blog/didact_mate/9.TiposdeInvestigación.Predictiva%2CProyectiva%2CInteractiva%2CConfirmatoriayEvaluativa.pdf
7. Welch S, Comer J (1988) Quantitative methods for public administration: techniques and applications, 2nd edn. Ill Dorsey Press, Chicago
8. Galvis Panqueva AH, del Pedraza Vega LC (2013) Desafíos del eLearning y del bLearning en educación superior: análisis de buenas prácticas en instituciones líderes. Cent. Innovación en Tecnol. y Educ. – Univ. los Andes., p 48 [Online]. https://conectate.uniandes.edu.co/images/pdf/desafios_conectate.pdf
9. Paur AB, Rosanigo ZB (2008) Objetos de Aprendizaje: factores que potencian su reusabilidad. XIV Congr. Argentino Ciencias la Comput., no. 02965, pp 1–12 [Online]. http://sedici.unlp.edu.ar/handle/10915/22004
10. Futures E (2013) Knowmad Society. Educ. Futur., pp 1–273 [Online]. http://www.knowmadsociety.com
11. Sánchez Domenech I, Rubia Avi M (2017) ¿Es posible la reconstrucción de la teoría de la educación de personas adultas integrando las perspectivas humanistas , críticas y postmodernas ?, Rev Electrónica Educ 21(2):1–26. https://doi.org/10.15359/ree.21-2.23
12. Knowles M (1977) Self-directed learning: a guide for learners and teachers. SELF-DIRECTED Learn. A Guid. Learn. Teach. Malcol m Knowles New York Assoc. Press. 1975. 135 pp., Pap. First Publ. June 1, 1977 Other https//doi.org/https://doi.org/10.1177/105960117700200220 Artic. Inf. No Access Artic. Informati, vol 2(2), pp 256–257. https://doi.org/10.1177/105960117700200220
13. UNESCO (2008) Organizaciones de las NAciones Unidad para la Educación, la Ciencia y la Cultura (UNESCO). La UNESCO y la Declaración Universal de Derechos Humanos. https://es.unesco.org/udhr
14. Plaza Arias JL, Constain Moreno G (2021) Experiencia de diseño de aplicaciones móviles basada en estrategias de gamificación para el fortalecimiento de habilidades cognitivas Mobile application design experience based on gamification strategies to. Rev Digit AIPO 2(1):17–24. [Online]. https://revista.aipo.es/index.php/INTERACCION/article/view/31/43
15. Morales Pacavita OS, Leguizamón González MC (2018) Teoría andragógica: aciertos y desaciertos en la formación docente en tic. Rev. Investig. y Pedagog. Maest. en Educ. Uptc 9:161–181. https://doi.org/10.19053/22160159.v9.n19.2018.7926
16. Galán Figueroa J, Venegas Martínez F (2016) Impacto de los medios electrónicos de pago sobre la demanda de dinero. Investig Económica 75(295):93–124. https://doi.org/10.1016/j.inveco.2016.03.003
17. Alves P (2020) MasterCard. Encuesta Mastercard: 63% de los chilenos quisiera poder realizar pagos en tiempo real. https://www.mastercard.com/news/latin-america/es/sala-de-prensa/comunicados-de-prensa/pr-es/2020/junio/encuesta-mastercard-63-de-los-chilenos-quisiera-poder-realizar-pagos-en-tiempo-real/
18. Hernández Sampieri R, Fernández Collado C, del Baptista Lucio MP (2005) Metodología de la Investigación. Mexico: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V
19. Páramo Bernal P (2013) La Investigación en Ciencias Sociales: estrategias de investigación. Univ. Pilot. Colomb., pp. 1–8 [Online]. https://books.google.com/books?hl=es&lr=&id=

2uk0DwAAQBAJ&oi=fnd&pg=PT75&dq=La+investigación+en+Ciencias+Sociales:+Estrategias+de+investigación.+&ots=SWIu17_QHM&sig=J87Vg2M_FApbK_l7ltLwGRgjR68

20. Plaza Arias JL (2021) Ambiente Virtual de Aprendizaje para la Formación en Seguridad Informática. Corporación Universitaria Comfacauca-Unicomfacauca

Automatic Jammer Signal Classification Using Deep Learning in the Spectrum of AI-Enabled CR-IoT

Muhammad Farrukh, Tariq Jamil Saifullah Khanzada, and Asma Khan

Abstract The emerging Internet of things (IoT) technology facilitates ubiquitous and seamless connectivity of various objects to provide different services. It is envisioned to incorporate self-awareness (SA) capabilities into the IoT devices to make the entire network autonomous and intelligent, giving the concept of cognitive radio (CR) CR-IoT network. Like other wireless networks, CR-IoT suffers from various kinds of abnormal attacks. However, due to the developments of deep learning models, it has become possible to efficiently recognize and classify malicious signals present in the signal transmission. In this work, we implemented deep learning models (AlexNet and GoogLeNet) to classify jammer signals present in a CR-IoT network using fast Fourier transform (FFT) and continuous wavelet transform (CWT) features extracted from the received orthogonal frequency division multiplexing (OFDM) signal spectrum. The CR-IoT network is considered in which users and a jammer are present. Both models are capable of classifying signals into the normal signal spectrum, jammer with high power, and jammer with low power. The performance of the proposed method is evaluated using receiver operating characteristic (ROC) curves.

Keywords Artificial intelligence (AI) · Deep learning · CR-IoT · OFDM · CWT

M. Farrukh (✉)
FAST-NUCES University, Karachi, Pakistan
e-mail: mfarrukh.shahid@nu.edus.pk

T. J. S. Khanzada
King Abdul Aziz University, Jeddah, Saudi Arabia

Mehran University of Engineering and Technology, Jamshoro, Pakistan

A. Khan
NED, University, Karachi, Pakistan
e-mail: tkhanzada@kau.edu.sa; asmakhan@neduet.edu.pk

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_36

1 Introduction

Machine learning (ML) methods have reshaped human life and revolutionized many fields such as Internet of things (IoT), vehicle-to-vehicle communication (V2V), 6G network, unmanned aerial vehicle (UAV), smart healthcare, intelligent transportation, and so forth. ML techniques are used for image classification, object detection, weather forecasting, abnormality detection from the spectrum of CR-IoT networks, time-series prediction, and many more [1]. However, the ML techniques have certain limitations. For instance, precise features must be selected, extracted from raw dataset, and then transformed into an appropriate representation vector from the raw dataset. Such features are then used to train an ML model to perform either classification or prediction tasks depending on the applications. On the contrary, deep learning (DL) methods have gained attention due to their ability to extract more complex and dense hidden features (spatial, temporal) from the raw data and retain powerful processing capabilities in generalizing the relationship of input data [2]. Moreover, deep learning models exhibit good performance on large-scale data, while machine learning models may encounter overfitting problems when dealing with a huge amount of data. This is due to the dense and complex architecture of deep learning models. DL models predict and cluster objects/items using a neural network (NN) composed of many layers of neurons trained on a given dataset. The intuition behind deep learning is an artificial neuron that mimics the human brain functionalities.

ML techniques have been implemented in communication systems to perform signal processing tasks at physical layer (PHY-Layer). Specifically, recent works also present many ML methods for the PHY-Layer CR-IoT network. Concurrently, DL methods have also evolved as one of the potential techniques and have been deployed to attain promising results in various CR-IoT applications. Signal processing techniques at PHY-Layer for communication systems contain strong foundations in information theory and statistics. These signal processing techniques use mathematical models that involve linearity and Gaussian statistics. However, many practical communication systems encounter nonlinearities issues that arise due to devices in either transmitter or receiver. To address such challenges, it is imperative to deploy DL, which does not require an explicit mathematical model and can achieve the optimal solution for nonlinear issues [3]. Moreover, due to the significant advancements in graphics processing unit (GPUs), it is now possible to realize complex and dense NN networks which are more energy efficient [4]. Moreover, DL methods are more robust in learning a full end-to-end communication system and can optimize the entire communication model in terms of signal processing [5]. Various DL architectures such as convolutional neural networks (CNNs), recurrent neural network (RNNs), and restricted Boltzmann machines have been implemented into multiple fields and obtained remarkable results. Specially, CNN network has gained significant attention in computer vision, image processing, and speech recognition. CNN networks have evolved from single NN that performs convolution operations on a given input in any of its layers. CNN architecture essentially consists of several layers:

pooling layer, convolution layer, and fully connected layer [6]. The sparse connectivity and parameter sharing characteristics of the convolutional layer have drastically improved the ML method's capabilities and performance. Deep learning methods have recently gained attention for signal classification, automatic modulation recognition, and normal and abnormal signals classifications [7]. In this perspective, the radio domain covering a broad range of networks from Bluetooth to 5G networks, classification operations help infer signal identification, determine the modulation type of a received signal, and discover abnormalities in the spectrum.

In this context, we considered a CR-IoT network in which mobile devices are communicating with a base station (BS) using OFDM modulated signals. A smart jammer is also hypothesized to be present in a network which launches malicious attacks with high and low power during the regular transmission as shown in Fig. 1. Such attacks disrupt normal communication and mislead the devices. Therefore, it is essential to perform classification operations to differentiate between normal and abnormal signals. Hence, deep convolutional neural networks (DCCN) have been used to accomplish classification tasks for the described scenario. In this work, two popular models (AlexNet [8] and GoogLeNet [9]) have been investigated and deployed. Motivated by the promising results of DL methods, following work has been carried out:

(a) Realize deep learning models (AlexNet and GoogLeNet) to classify normal user transmission and jammer attacks (with high and low power) inside the CR-IoT spectrum.

(b) Collection of two features sets of the OFDM modulated signal transmission. One set is obtained using CWT technique in terms of scalograms to represent spectrum contents in the form of an images. At the same time, the second set is obtained using FFT, which gives complex data samples. These samples are then converted into the images to be used in the training of DL models.

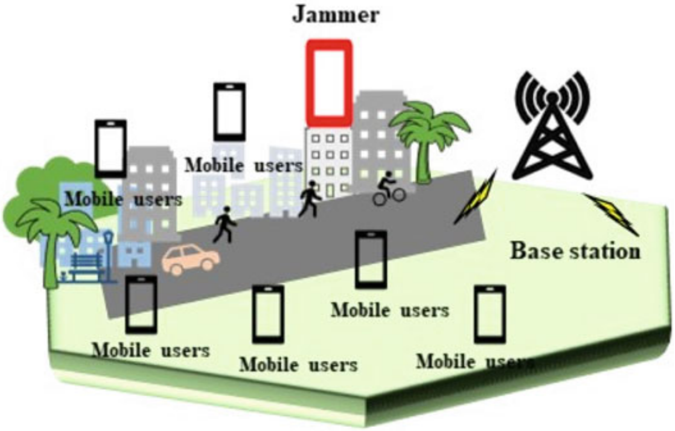


Fig. 1 CR-IoT network comprises of a base station, cognitive mobile users, and a jammer

(c) DL models are trained on FFT and CWT datasets. After training, a test set is applied, and the performance of trained models is evaluated using ROC curves.

2 Literature Review

There has been a lot of work proposed and developed to perform radio signal classification by the researcher community. In this perspective, Ref. [5] presents an end-to-end learning model for radio signal recognition. Signal identification for intelligent radios is demonstrated and discussed in [10]. Zheng et al. [11] proposed signal classification method for cooperative radio classification. According to the recent advancements and developments in the signal classification domain, classification techniques are categorized based on state estimation, feature extraction, and DL model-based approach. In [12], authors proposed autocorrelation-based convolutional network for automatic modulation classification using deep learning method. In [13], modulation techniques such as binary phase shift keying (BPSK), quadrature phase shift keying (QPSK), frequency shift keying (FSK), and minimum shift keying (MSK) have been classified using S-transform-based features. In [14], authors presented a work which deploys a wavelet transform and an artificial neural network (ANN) classifier to track audio frequency in a network. In [15], cyclostationary features are used for detecting and classifying of OFDM, quadrature amplitude modulation (QAM), and offset quadrature amplitude modulation (OQAM) signals. Li et al. [16] demonstrated deep learning model for modulations (FSK, PSK, MSK, and QAM) identification. In [17], high order cumulants are used to learn deep learning model to perform modulation recognition. Tang et al. [18] described a method which uses a DL model generative adversarial network (GAN) to automatically recognize modulation in cognitive radio network. Wang et al. [19] presented a data-driven approach which deploys CNN model for automatic modulation recognition in a CR. In view of the foregoing research works, DL methods can be deployed to classify legitimate and jammer signals in the CR-IoT network spectrum.

3 System Model

We considered a CR-IoT network in which mobile devices are communicating with a base station (BS) using OFDM modulated signals. A smart jammer is also hypothesized to be present in a network which launches malicious attacks during the regular transmission. Such attacks disrupt normal communication and mislead the devices. Therefore, it is essential to perform classification operations to differentiate between normal and abnormal signals. Hence, a deep convolutional neural network (DCCN) has been used to accomplish classification tasks for the described scenario. In this work, two popular models (AlexNet and GoogLeNet) are investigated and deployed. CWT transforms OFDM signals into scalograms, which represent images encoding time and frequency information of the spectrum. Scalograms are obtained by taking absolute value of CWT signal coefficients. CWT transforms OFDM signals into scalograms, which represent images encoding time and frequency information of the spectrum. CWT filter bank is computed first to create the scalograms. Before acquiring the scalograms, the filter bank is deployed to obtain the CWT of the 1000 successive samples of the OFDM data. After that, scalograms are obtained from the coefficients. The generated scalogram is transformed into red green blue (RGB) images. The second dataset is obtained using FFT transform. FFT operation provides complex samples of OFDM signals. It is necessary to convert complex data samples obtained after applying Fourier transformation into RGB images.

4 Implementation

The implementation phase consists of training and testing phases is shown in Fig. 2. Parameters of both models are modified according to the given scenario and problem in this work. The models are capable of classifying spectrum signals into the following classes: Reactive jammer with high power (RJHP), reactive jammer with low power (RJLP), and normal signal spectrum (NSS). Accordingly, for AlexNet, the number of the output layer is taken three instead of the default number, which is 1000. The other configuration parameters are set as mini-batch size 64 with learning rate 0.0001, and 227 × 227 image resolution is taken for AlexNet. Adaptive moment estimation (ADAM) is used as a learning method for both models as it combines the benefits of root mean squared propagation (RMSPro) and momentum method and achieved high classification accuracy in comparison with stochastic gradient descent

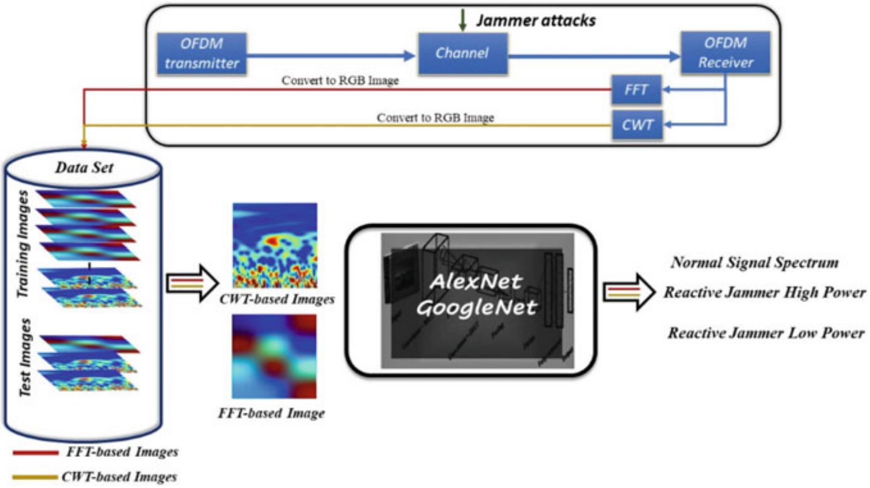


Fig. 2 Deep learning models with FFT and CWT images used to classify jammer signals

method (SGDM) and RMsProp. For GoogLeNet, input image resolution is 224 × 224, and mini-batch size 64 with learning rate 0.0001 are selected. The training of both models follows the given steps: (a) Obtain the time–frequency representation of the OFDM modulated signals using CWT and FFT techniques and convert the generated data into RGB images. (b) Each generated image is labeled according to the classes. (c) For training, 70% images per signal category are collected, and for testing, 30% labeled images per signal category. The training is done using the computing system NVIDIA GEFORCE CPU CORE i7. After the models have been trained, a test set is applied to infer the performance. The performance of models is analyzed in terms of the ROC curves.

5 Simulation and Results

To test the performance of both models (AlexNet and GoogLeNet), two datasets, namely FFT-based images dataset, and CWT-based images dataset, are utilized to conduct the experiments. Both models' performance on two datasets is evaluated using a classification accuracy plotted against various SNR values as shown in Fig. 3 (left figure) for FFT-based image dataset and Fig. 3 (right figure) CWT-based image dataset. It can be observed from Fig. 3 (left figure) that the classification accuracy of AlexNet model was slightly better than the GoogLeNet for FFT-based image dataset. On the other hand, for CWT-based image dataset, GoogLeNet classification accuracy, was more nuanced than the AlexNet, as depicted in Fig. 3 (right figure). Figure 4 presents comparison analysis between the deployed models and simple CNN models (trained on both datasets). It can be observed that both DL models outperform the simple CNN models. Classification accuracy comparison is plotted at various SNR values for all three models on both datasets. It can be analyzed that at

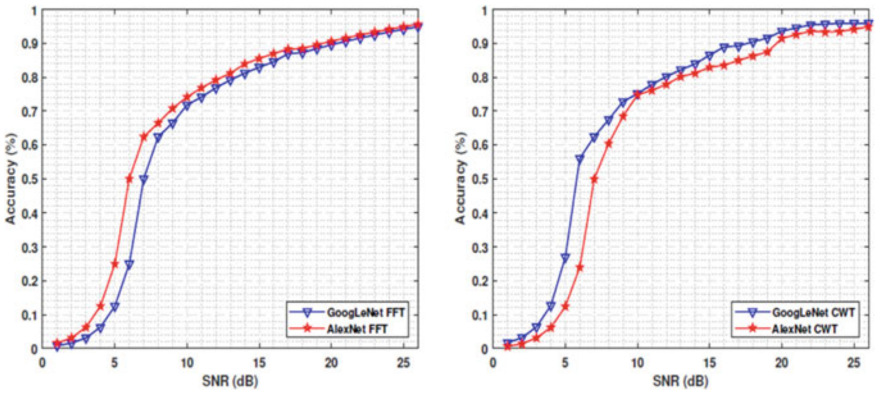


Fig. 3 Accuracy plots left figure ALexNet and GoogLeNet models performance on FFT-based images right figure ALexNet and GoogLeNet models performance on CWT-based images

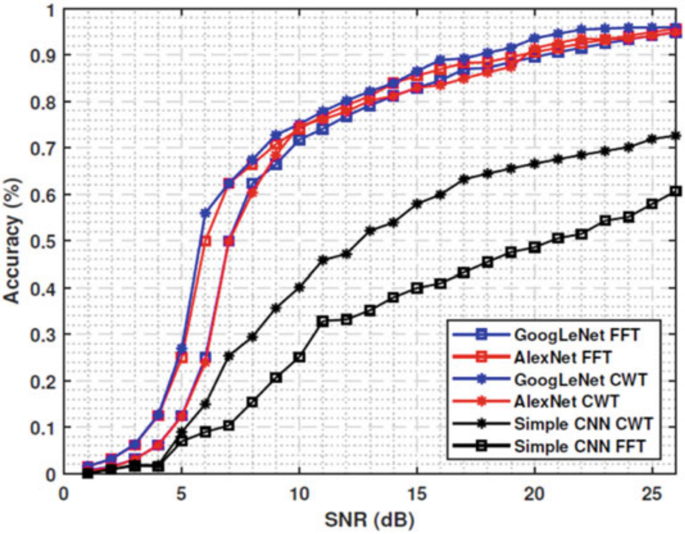


Fig. 4 Performance comparison of AlexNet and GoogLeNet with conventional CCN model on FFT and CWT-based images

20 dB SNR, AlexNet performance was better than the GoogLeNet on FFT- dataset, and GoogLeNet had better classification accuracy than AlexNet on CWT dataset. However, a simple CNN did not perform well on both datasets.

Hence, we can deduce the following conclusion from the implemented method:

Classification of abnormal signals (jammer attacks) can be achieved using either of the deep learning models. However, the input data's pre-processing technique for training the DL model is crucial and must be selected according to the application.

As presented in this work, there is a slight difference in model performance on both datasets. Therefore, it is exceptionally motivating to use the FFT-based images dataset. This is because most recent wireless technologies, such as wireless fidelity (WiFi), long-term evolution (LTE), 5G, 6G, and CR-IoT networks, etc., deploy OFDM as a potential modulation technique due to its various advantages. Moreover, the OFDM communication system contains a built-in FFT-module. Thus, it is easy to extract FFT information in the OFDM system receiver without deploying any other transformation technique. Such information can then be converted into RGB images and use to train the DL model as presented in this work. Hence, we can avoid extra processing in terms of time and power in calculating scalograms of the received OFDM signal. Instead, we can readily extract FFT information and deploy either of the DL models to accomplish classification tasks.

6 Conclusion and Future Work

In this work, we presented a deep learning model implementation to recognize normal and abnormal received OFDM signals in a CR-IoT network. The proposed method uses FFT and CWT features for the training of the deep learning models and classify signals into normal, jammer with high power, and jammer with low power. The results showed that deep learning models can classify abnormalities (jammer attacks) present in the spectrum. As a future, short-time Fourier transform (STFT) will be considered to train the deep learning models to perform classification tasks.

References

1. Ma X, Yao T, Hu M, Dong Y, Liu W, Wang F, Liu J (2019) A survey on deep learning empowered IoT applications. IEEE Access 7(181):721–181, 732
2. Gjoreski M, Gams MŽ, Luštrek M, Genc P, Garbas J, Hassan T (2020) Machine learning and end-to-end deep learning for monitoring driver distractions from physiological and visual signals. IEEE Access 8:70590–70603. https://doi.org/10.1109/ACCESS.2020.2986810
3. Nishizaki H, Makino K (2019) Signal classification using deep learning. In: 2019 IEEE international conference on sensors and nanotechnology, pp 1–4
4. Selvaluxmiy S, Kumara TN, Keerthanan P, Velmakivan R, Ragel R, Deegalla S (2016) Accelerating k-NN classification algorithm using graphics processing units. In: 2016 IEEE international conference on information and automation for sustainability (ICIAfS), pp 1–6. https://doi.org/10.1109/ICIAFS.2016.7946528
5. Kulin M, Kazaz T, Moerman I, De Poorter E (2018) End-to-end learning from spectrum data: a deep learning approach for wireless signal identification in spectrum monitoring applications. IEEE Access 6:18 484-18 501
6. Dileep P, Das D, Bora PK (2020) Dense layer dropout based CNN architecture for automatic modulation classification. In: 2020 national conference on communications (NCC), 2020, pp 1–5. https://doi.org/10.1109/NCC48643.2020.9055989
7. Bu K, He Y, Jing X, Han J (2020) Adversarial transfer learning for deep learning based automatic modulation classification. IEEE Signal Process Lett 27:880–884
8. Mashrur FR, Dutta Roy A, Saha DK (2019) Automatic identification of arrhythmia from ECG using AlexNet convolutional neural network. In: 2019 4th international conference on electrical information and communication technology (EICT), pp 1–5
9. Salavati P, Mohammadi HM (2018) Obstacle detection using GoogleNet. In: 2018 8th international conference on computer and knowledge engineering (ICCKE), pp 326–332
10. Dobre OA (2015) Signal identification for emerging intelligent radios: classical problems and new challenges. IEEE Instrum Meas Mag 18(2):11–18
11. Zheng S, Chen S, Yang X (2019) Deep Learning for cooperative radio signal classification, eprint={1909.06031}, archivePrefix ={arXiv}, primaryClass ={eess.SP}
12. Zhang D, Ding W, Wang H, Zhang B (2020) Autocorrelation convolution networks based on deep learning for automatic modulation classification. In: 2020 15th IEEE conference on industrial electronics and applications (ICIEA), pp 1561–1565. https://doi.org/10.1109/ICIEA48937.2020.9248386
13. Satija U, Mohanty M, Ramkumar B (2015) Automatic modulation classification using S-transform based features. In: 2015 2nd international conference on signal processing and integrated networks (SPIN), pp 708–712
14. Havryliuk V (2019) Audio frequency track circuits monitoring based on Wavelet transform and Artificial Neural Network classifier. In: 2019 IEEE 2nd Ukraine conference on electrical and computer engineering (UKRCON), pp 491–496

15. Vukotić S, Vućić D (2015) Detection, and classification of OFDM/QAM and OFDM/OQAM signals based on cyclostationary features. In: 2015 23rd telecommunications forum Telfor (TELFOR), pp 232–235
16. Li J, Qi L, Lin Y (2016) Research on modulation identification of digital signals based on deep learning. In: 2016 IEEE international conference on electronic information and communication technology (ICEICT), pp 402–405
17. Xie W, Hu S, Yu C, Zhu P, Peng X, Ouyang J (2019) Deep learning in digital modulation recognition using high order cumulants. IEEE Access 7:63 760–6766
18. Tang B, Tu Y, Zhang Z, Lin Y (2018) Digital signal modulation classification with data augmentation using generative adversarial nets in cognitive radio networks. IEEE Access 6:15 713–15 722
19. Wang Y, Liu M, Yang J, Gui G (2019) Data-driven deep learning for automatic modulation recognition in cognitive radios. IEEE Trans Veh Technol 68(4):4074–4077

Arm-Z as a Modular Tracking Device

Ela Zawidzka, Jacek Szklarski, and Machi Zawidzki

Abstract Arm-Z is a hyper-redundant manipulator based on a sequence of linearly joined identical modules. Each module has only one degree of freedom—a twist relative to the previous module. Arm-Z can be potentially economical, as the modules can be mass-produced. Arm-Z is also robust, as the malfunctioning module can be replaced. Moreover, if some modules malfunction, the device can still execute tasks with certain accuracy. However, the disadvantage of Arm-Z is a non-intuitive and difficult control. This paper presents a concept of a modular tracking device comprised of four identical modules. As an example, the Sun-tracking setup is used with possible application for solar energy harvesting.

Keywords Extremely modular system · Arm-Z · Hyper-redundant manipulator · Sun-tracking

1 Introduction

Snakes are supremely adapted for various habitats. This is due to the redundancy of the snake mechanism. In some cases of non-regular environments, the biology-inspired trunk-like robot can outperform conventional robot mobility (e.g. legged, tracked or wheeled). The research on snake-like robots commenced already several decades ago. The locomotion of snakes was systematically studied as early as 1940s [1]. A half of a century later, the mathematical model was introduced. In 1993 trunk-like manipulators and locomotors were proposed in [2]. This type of manipulators have distinct characteristics of motion. This gives them particular advantage in conditions where conventional robotic manipulators are impractical. Snake/trunk-like manipulator can place working head in a complicated space which is inaccessible by other methods. The range of reach of such manipulators is relatively large (tens of metres). Most importantly, such manipulators can operate in unsafe environments.

E. Zawidzka (✉) · J. Szklarski · M. Zawidzki
Institute of Fundamental Technological Research, Polish Academy of Sciences, Warsaw, Poland
e-mail: zawidzka@ippt.pan.pl

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_37

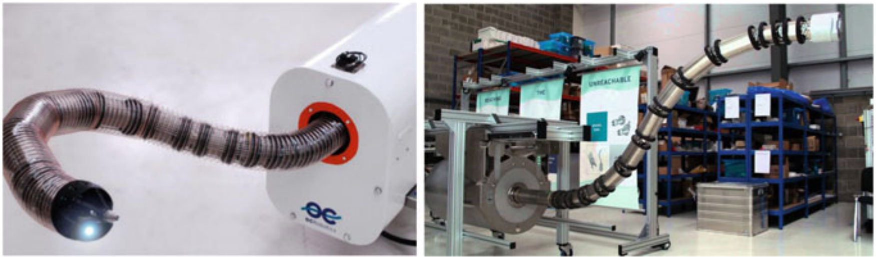


Fig. 1 Two examples of robotic trunk-like manipulators offered by Oliver Crispin Robotics Ltd. (http://www.ocrobotics.com)

Depending on the working head installed at the tip of such manipulator, it can weld, clean, serve for visual inspection etc. There are only a few enterprises offering this type of manipulator; the available solutions are scarce and mostly experimental (for examples, see Fig. 1)

In addition, snake/trunk-like robotic arms can have considerably larger numbers of degrees of freedom (DOFs). This contrasts with conventional industrial manipulators which have low number of DOF. In the case of Arm-Z manipulator, its DOF number equals to the number of linearly assembled units -1. Redundant number of DOFs allows not only the ability of executing complex movements, but also substantially improves the robustness and fault tolerance. This is in alignment with the idea of so-called hyper-redundant manipulators (HRM for short, [3]). Due to the high non-linear characteristics of the HRM, its advantage comes at the cost of very difficult and counter-intuitive controlling. For example, the control of a *bionic trunk* requires quite intensive application of AI (artificial intelligence) techniques [4–6], while the control of a typical industrial manipulator is straightforward, as its inverse kinematic problem can be solved easily [7]. For more details on hyper-redundant robotic arms, see [8]. The idea of extreme modularization is novel and still fairly unexplored. The research on structural optimization of modular constructions is also comparatively scarce. As an example, Ref. [9] presents a multi-objective optimization of a set of a number of vehicle structures at the level of common beam parts. Another example of a layout optimization of a modular bridge, where the design variables are effectively discrete and encode the choice from a predefined set of local module topologies has been presented in [10].

2 The Idea of Arm-Z

Complicated 3D tubular shapes may be constructed with comparatively uncomplicated identical modules [11]. Reference [12] introduced a parametric design system composed of congruent units. The idea of Arm-Z robotic manipulator is based on assembly of congruent units. Each unit has one degree of freedom (1-DOF), namely

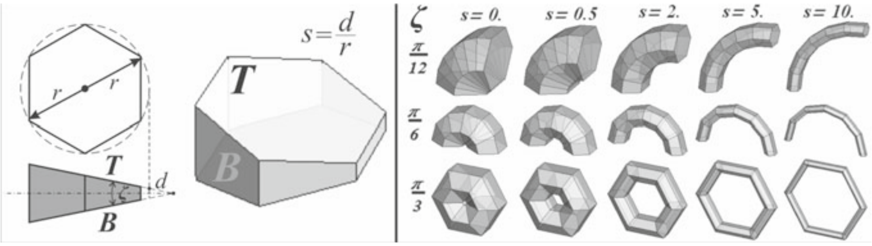


Fig. 2 On the left: visualization of Arm-Z module which is defined by the following parameters: r, d, ζ and $k = 6$ (hexagon) and its isometric view. On the right: examples of simple assembly of modules with various combinations of their geometrical parameters

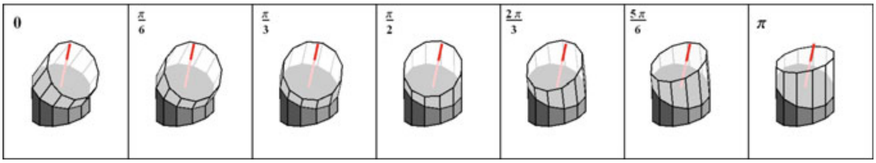


Fig. 3 The relative rotations of Arm-Z unit. The bottom module is fixed and shown in grey. Red line indicated the axis of rotation for the next module in the sequence

a twist relative to the previous unit [13]. The emerging behaviour of Arm-Z manifested by complex movements in 3D results from simple alterations of these relative twists, which can be discrete or continuous.

The modules of Arm-Z are geometric entities analogue to sectors of circular tori. All modules are defined by the following parameters: size r, offset d, number of sides k and ζ, that is the angle between upper (**T**) and lower (**B**) planes of the module. These parameters are illustrated in Fig. 2.

The shape of entire Arm-Z structure depends on the number of units, their geometric parameters and the relative rotations among the modules. As an example, two Arm-Z units at six successive discrete rotations from 0 to π are shown in Fig. 3.

The operational space depends on the number of modules. It forms a complex three-dimensional surface with voids. Therefore, generally, the tip of Arm-Z cannot reach every point in three-dimensional space constrained by its theoretical range, but it can reach certain points with some tolerance, as illustrated with volumetric renderings in Fig. 4.

3 The Sun-tracking Task

As an example of a steady movement of the manipulator following given direction, we propose a Sun-tracking device with possible application, e.g. for solar energy harvesting. Figure 5 shows the position of the Arm-Z in the coordinate system and

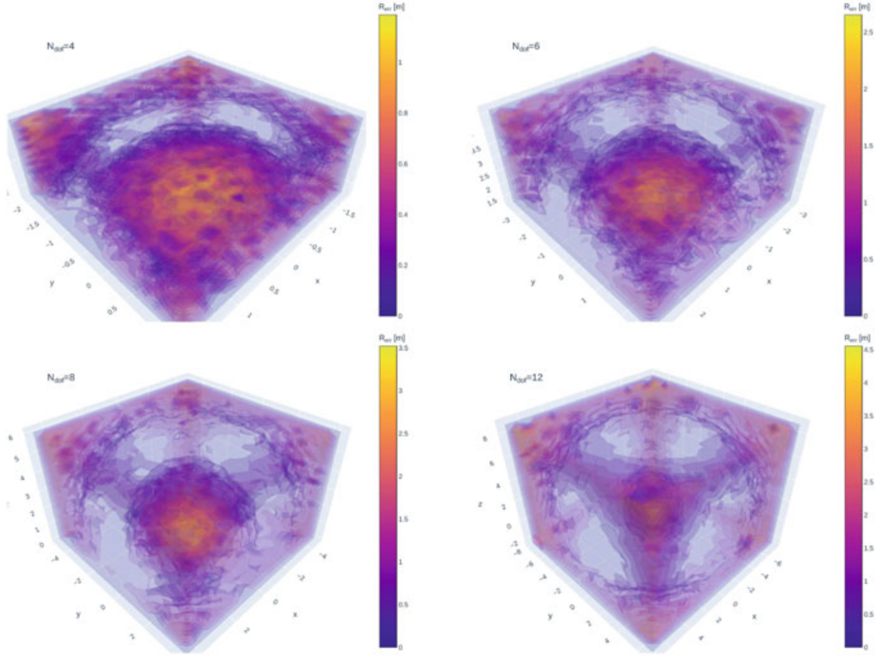


Fig. 4 Volumetric renderings showing surfaces of reaching error for various N_{dof}. It is clear that the largest errors are close to the base of the Arm-Z structure and in the corners of the bounding box

explains the tracking parameters. $\mathbf{V_N}$ is the normal vector to the surface of the last module; in other words, it is a vector pointing from the tip of the manipulator. $\mathbf{V_d}$ stands for the desired direction of the normal vector (in this case, the sunlight direction). $\mathbf{V_d}(\phi, \theta)$ is defined by the azimuth ϕ and altitude θ. In this task, $\mathbf{V_N}$ must follow $\mathbf{V_d}$; in other words, the angle between these two vectors is minimized. $\mathbf{P_t}$ is the position of the tip of the manipulator. N_{dof} is the number of degrees of freedom of the system; it is equal to the number of modules—1.

In this task, the intention is to follow the Sun direction during summertime (from summer solstice to September equinox) between 10 a.m. and 6 p.m., as illustrated in Fig. 6.

The angular errors for manipulators of various numbers of degrees of freedom: 1, 2, 3, 4, 6 and 7 are shown in Fig. 7. White line indicates that there the horizontal plane. Black indicates very small errors. Already a 4-module manipulator can cover almost all desired directions. The last figure shows that 7 degrees of freedom allow to cover almost all directions in 3D space (including the space below the manipulator).

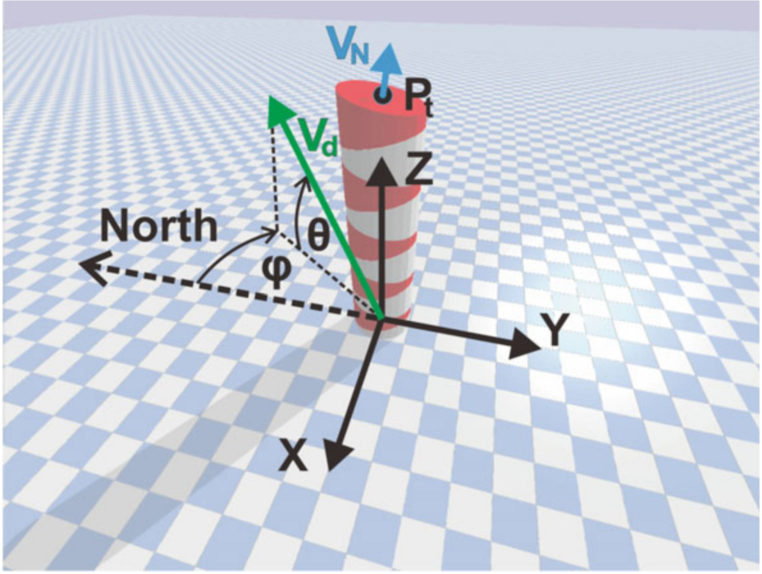


Fig. 5 The coordinate system, notation and the control parameters

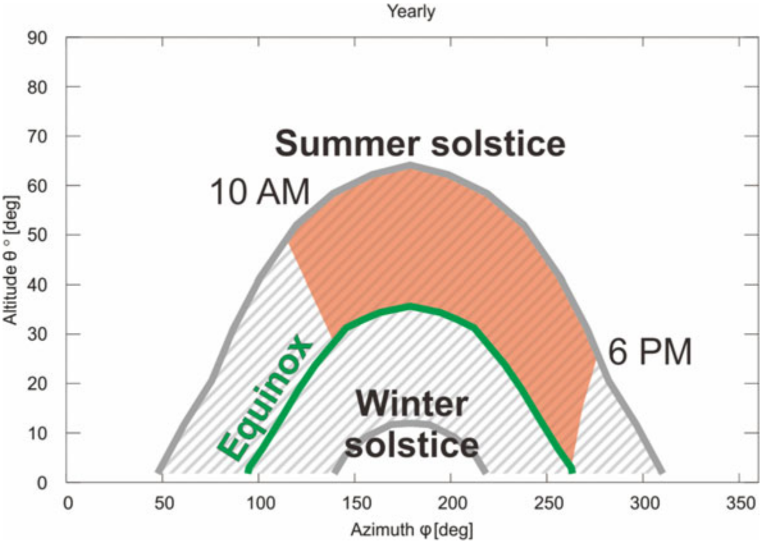


Fig. 6 Possible Sun location during a year and for the given periods during summertime (indicated in red)

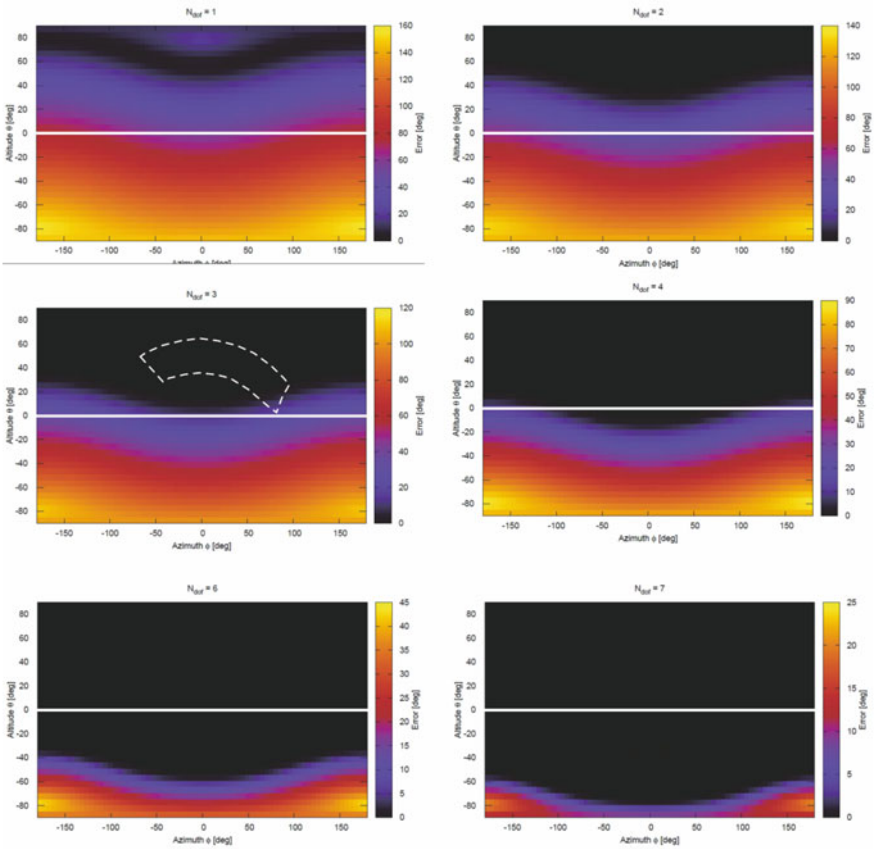


Fig. 7 Visualization of the angular errors for Arm-Z manipulators of various numbers of degrees of freedom: 1, 2, 3, 4, 6 and 7. The outline indicating the tracking period from Fig. 6 is superimposed as the white dashed line for the case of 3 DOF

3.1 The Optimization of the Tracking Action

In order to perform realistic simulations, the manipulator has been implemented in Bullet Physics SDK [14]. It is a widely used tool for real-time collision detection and multi-physics simulation for virtual reality (VR), robotics, machine learning etc. In order to control the manipulator, the inverse dynamics has been solved by two numerical methods: the classical recursive Newton Euler algorithm (RNEA), [15] and by means of dual annealing [16, 17]. As it turned out, the latter method performed better (in terms of average errors) than RNEA. This can be attributed to the fact that the system is highly non-linear, and even small changes in position of modules at the bottom can profoundly influence the tip position.

In order to continuously control the manipulator, the twist velocities and spins of three modules have been optimized with the dual annealing method in a way in

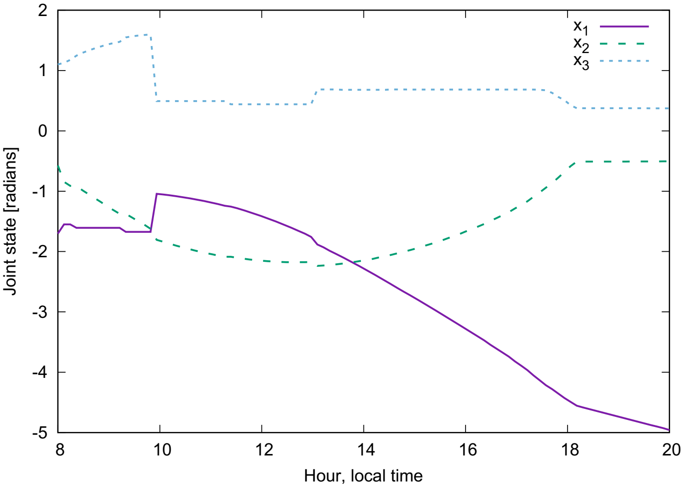


Fig. 8 Joint states x_1, x_2, x_3 for a four-module structure which follows the sun on July 1st between 8 a.m. and 8 p.m. local time

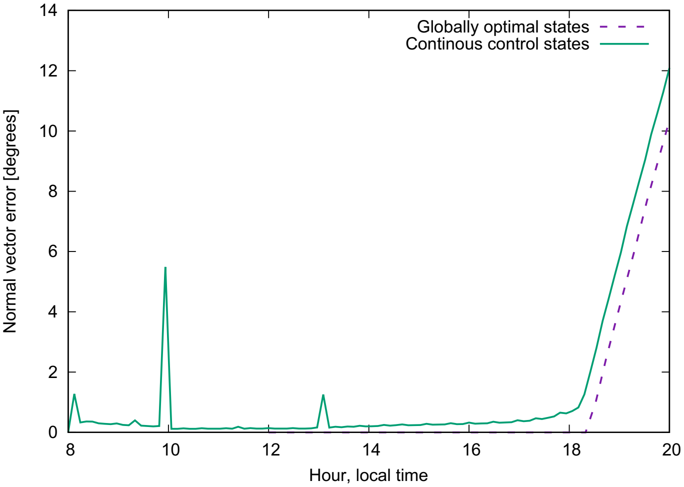


Fig. 9 Error (angle between $\mathbf{V_d}$ and $\mathbf{V_N}$) for globally optimal states and for the continuous control scenario (some peaks can be noticed for the latter). From Fig. 7, it follows that the tips normal vector $\mathbf{V_N}$ cannot follow the Sun for low latitudes, especially during sunrise/sunset. Hence, the growing error from approximately 6 p.m

which significant deviations from the current state have been penalized. This made possible to achieve a quite smooth movement of the manipulator. The results (angular velocities of the individual modules) are shown in Fig. 8.

Figure 9 shows the angular errors throughout the tracking period.

4 Conclusions

- Effective direction-tracking in given task is already possible with only four modules (of which three are moving, thus three DOF).
- The precision of direction-tracking in this simple example is satisfactory.

5 Future Work

- Improvement of the control
- Development of larger Arm-Z for more demanding tasks
- Building a prototype

Acknowledgements This research is a part of the project titled *Arm-Z: an extremely modular hyperredundant low-cost manipulator—development of control methods and efficiency analysis* and funded by *OPUS 17* research grant No. 2019/33/B/ST8/02791 supported by the National Science Centre, Poland.

References

1. Gray J (1946) The mechanism of locomotion in snakes. J Exp Biol 23(2):101–120
2. Hirose S (1993) Biologically inspired robots: snake-like locomotors and manipulators. Oxford University Press
3. Ning K, Wörgötter F (2009) A novel concept for building a hyper-redundant chain robot. IEEE Trans Robot 25(6):1237–1248
4. Rolf M, Steil JJ (2014) Efficient exploratory learning of inverse kinematics on a bionic elephant trunk. IEEE Trans Neural Netw Learn Syst 25(6):1147–1160
5. Melingui A et al (2014) Qualitative approach for forward kinematic modeling of a compact bionic handling assistant trunk. IFAC Proc 47(3):9353–9358
6. Falkenhahn V, Hildebrandt A, Neumann R, Sawodny O (2017) Dynamic control of the bionic handling assistant. IEEE/ASME Trans Mechatron 22(1):6–17
7. Murray RM, Li Z, Shankar Sastry S, Shankara Sastry S (1994) A mathematical introduction to robotic manipulation. CRC Press
8. Chirikjian GS, Burdick JW (1994) A hyper-redundant manipulator. IEEE Robot Automat Mag 1(4):22–29
9. Torstenfelt B, Klarbring A (2006) Structural optimization of modular product families with application to car space frame structures. Struct Multidiscip O 32(2):133–140
10. Tugilimana A et al (2017) Conceptual design of modular bridges including layout optimization and component reusability. J Bridge Eng 22 (11)
11. Fuhs W, Stachel H (1988) Circular pipe-connections. Comput Graph 12(1):53–57
12. Zawidzki M, Nishinari K (2013) Modular pipe-z system for three-dimensional knots. J Geometry Graph 17(1):81–87
13. Zawidzki M, Nagakura T (2014) Arm-Z: a modular virtual manipulative. In: Schröcker H-P (ed) Proceedings of the 16th international conference on geometry and graphics, pp 75–80
14. Coumans E, Bai Y, Pybullet, a python module for physics simulation for games, robotics and machine learning. http://pybullet.org, 2016–2021

15. Luh JYS, Walker MW, Paul RPC (1980) On-line computational scheme for mechanical manipulators. J Dyn Syst Measur Control 102(2):69–76. https://doi.org/10.1115/1.3149599. ISSN 0022-0434
16. Xiang Y, Sun DY, Fan W, Gong XG (1997) Generalized simulated annealing algorithm and its application to the thomson model. Phys Lett A 233(3):216–220. https://doi.org/10.1016/S0375-9601(97)00474-X. ISSN 0375-9601
17. Virtanen P, Gommers R, Oliphant TE, Haberland M, Reddy T, Cournapeau D, Burovski E, Peterson P, Weckesser W, Bright J, van der Walt SJ, Brett M, Wilson J, Jarrod Millman K, Mayorov N, Nelson ARJ, Jones E, Kern R, Larson E, Carey CJ, Polat I, Feng Y, Moore EW, VanderPlas J, Laxalde D, Perktold J, Cimrman R, Henriksen I, Quintero EA, Harris CR, Archibald AM, Ribeiro AH, Pedregosa F, van Mulbregt P, SciPy 1.0 Contributors (2020) SciPy 1.0.: fundamental algorithms for scientific computing in python. SciPy 1.0. Nat Methods 17:261–272. https://doi.org/10.1038/s41592-019-0686-2

Epidemiological Profile of Cutaneous and Visceral Leishmaniasis in the City of Meknes, During the Period from 2014 to 2019

Abdelfatah Benchahid, Driss Belghyti, Zakaria Zgourdah, Omar Lahlou, Said Lotfi, and Khadija El Kharrim

Abstract *Introduction* Leishmaniasis is a common parasitosis of humans and animals. They are caused by flagellated protozoa belonging to the genus Leishmania and transmitted to humans by the bites of insect vectors, called female sandflies. They are the second most common cause of parasitic death worldwide after malaria and are endemic in Asian and African countries. In Morocco, they pose a real public health problem. The objective of our work is to analyse the spatial and temporal distribution of cutaneous and visceral leishmaniasis in order to evaluate the epidemiological situation of these parasitoses in the region of Meknes and to appreciate their evolution according to the nature of the environment. *Material and method* In this context, we conducted a retrospective study during the period from 2014 to 2019, collecting all cases of leishmaniasis reported in this city. Epidemiological data were collected from the registers of new cases of leishmaniasis at the service of infrastructure and ambulatory actions of the provincial and prefectural delegation of the Ministry of Health of Meknes. *Results* A total of fifty-four new cases were declared infected, these data shows that there is coexistence of both forms of leishmaniasis: cutaneous (79.63%) and visceral (20.37%) with a predominance of rural areas (61.11%), as well as, the sex ratio was 0.86 and the average annual incidence was 9 cases per year. *Conclusion* The major challenge for Morocco between now and 2030 is the definitive elimination of leishmaniasis, which requires the adoption of a global approach by acting on the sources of contamination through surveillance and appropriate management, effective control of vectors and reservoirs, and innovative strategies to raise awareness in local society.

Keywords Cutaneous leishmaniasis · Visceral leishmaniasis · Sandfly · Epidemiological profile · Retrospective study · Meknes

A. Benchahid (✉) · D. Belghyti · Z. Zgourdah · S. Lotfi · K. El Kharrim
Faculty of Science, Laboratory: Natural Resources and Sustainable Development, Ibn Tofail University, Kenitra, Morocco
e-mail: Abdelfatah.benchahid@uit.ac.ma

O. Lahlou
Services of the Prefectural Ambulatory Action Infrastructures, Kenitra, Morocco

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_38

1 Introduction

Leishmaniasis is a parasitic disease that is widespread on the surface of the earth and has a generally circumterranean distribution [1, 2]. It represents a real health problem in tropical countries due to their clinical (cutaneous, visceral and cutaneous-mucosal) and epidemiological diversity, the complexity of its parasitic cycle and the multiplicity of its reservoirs (human, rodent and dog). It is transmitted to humans by the bite of small infested sandflies: female sandfly. This insect is well adapted to tropical and subtropical climates and is found in the Mediterranean region [3, 4]. Leishmaniasis manifests itself in three different forms: cutaneous, visceral or mucocutaneous and has territories whose delimitation depends on intrinsic factors related to the species of parasite, vector sandflies and reservoir mammals, but also on extrinsic, environmental factors, particularly the insalubrity of spaces [1]. Global prevalence exceeds 10 million cases, there are 1.5–2 new cases per year, a high proportion of which are children, and annual global mortality is 70,000, the second highest cause of parasitic death after malaria.

In Morocco, leishmaniasis is the first group of vector-borne parasitic diseases and is a notifiable infectious disease according to the ministerial decree N° 683–95 of 31 March 1995. Despite this regulation, these infections pose a real public health problem, due to the increasing number of cases detected each year and the extension of cutaneous leishmaniasis to other areas previously free of it [5–7] as well as the appearance of visceral leishmaniasis cases. In this sense, studies have been carried out in some Moroccan cities, namely, Marrakech, Bni Mellal, Boulmane, Moulay Yaakoub and El Hajeb. To our knowledge, no epidemiological study concerning cases of cutaneous and visceral leishmaniasis has been carried out in this region of Meknes which is located adjacent to endemic areas such as Fez, Moulay Yaakoub and Sidi Kacem. For this reason, an epidemiological study would be necessary in the city of Meknes to determine and clarify the epidemiological situation of parasitosis on the one hand, and on the other hand, to help the hygiene service involved in the fight against vectors to better carry out control and prevention actions.

The objective of this retrospective study is to analyse the spatio-temporal distribution of cutaneous and visceral leishmaniasis in order to evaluate the epidemiological profile of these parasites in the region of Meknes.

2 Materials and Methods

2.1 Study Environment

This work is conducted within the region of Meknes, covering an area of 1786 km^2 according to the 2015 administrative division, and characterized by two major geographical areas, namely: the Saïs plateau and the pre-Rifa hills of Zerhoun, as well as a semi-continental climate of the Mediterranean type, with cool, rainy winters and

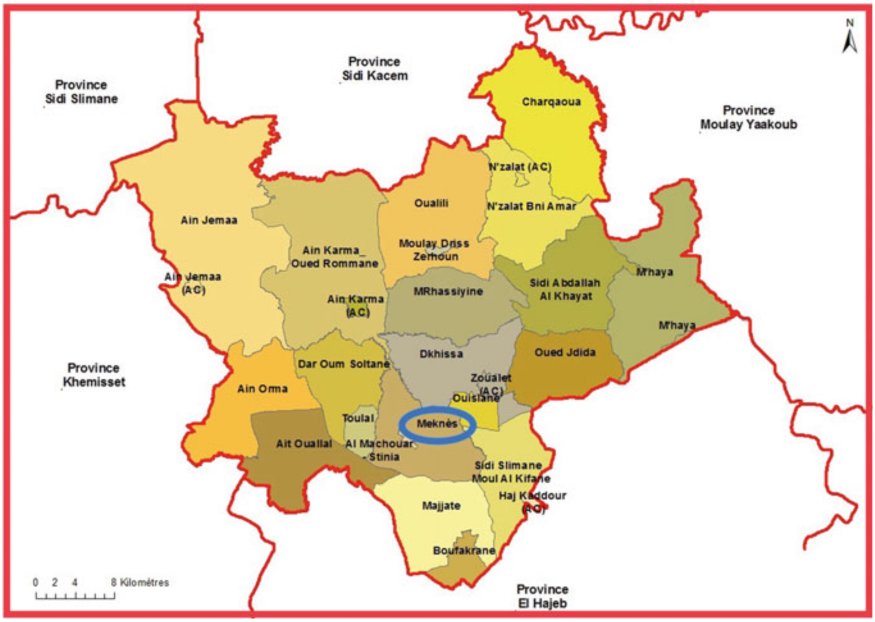


Fig. 1 Geographical map of the Meknes region (https://www.hcp.ma/region-meknes/RGPH-en-cartes_a106.html)

hot, dry summers, according to the 2014 General Census of Population and Housing, the legal population of the prefecture reached 835,695 inhabitants in 2014 compared to 715,285 in 2004. Thus, it recorded an average annual growth rate of 1.6% for the period 2004–2014. This rate is higher than those recorded at the regional (0.9%) and national (1.3%) levels. As a result, the demographic growth of the last decade has led to the construction of precarious housing on the outskirts of the prefecture of Meknes and within the urban fabric. The prefectural territory of the region is composed of 6 urban and 15 rural communes representing, respectively, 18.2% and 9.3% of the total of the same type of commune at the level of the Fez - Meknes region [8] (Fig. 1).

2.2 Materials and Methods

The present study included all new cases of cutaneous (LC) and visceral (LV) leishmaniasis recorded during the period 2014–2019. Indeed, the data for this retrospective study were taken from the epidemiological bulletins published in the official website of the Ministry of Health in figures from 2015 to 2019 (Moroccan Ministry of Health, 2014–2018). However, these documents only report the total number of leishmaniasis cases reported in the region of Meknes without distinguishing between the types of leishmaniasis nor the socio-demographic characteristics of the infected persons such as: age, sex, living environment (rural or urban), classification of cases (autochthonous, imported, paradoxical) and type of screening (positive or negative). For this, we completed the data of our study by collecting them from the case registers of the SIAAP service of the delegation of the Ministry of Health in Meknes.

We then analysed the epidemiological data and interpreted the results obtained in various statistical forms such as tables, graphs or curves, and started to calculate the incidence rate of leishmaniasis, which corresponds to the number of new cases detected per hundred thousand inhabitants in a given exposed population in one year.

The statistical analysis was carried out for all the data collected and recorded on grids by using Excel software (Microsoft) version 2010, which allowed us to diagnose and interpret the epidemiological results concerning the leishmaniasis disease in the region of Meknes.

Regarding the impact of this study in the long term, our study aims to decrease the new cases of cutaneous and visceral leishmaniasis and eventually eliminate this parasitosis from our study area.

We can also use this retrospective study for all parasitic diseases such as malaria.

3 Results and Discussion

3.1 Annual Distribution of Leishmaniasis According to Environment

The results of our retrospective study of the annual incidence of leishmaniasis, during the period 2014–2019, are shown in Fig. 2.

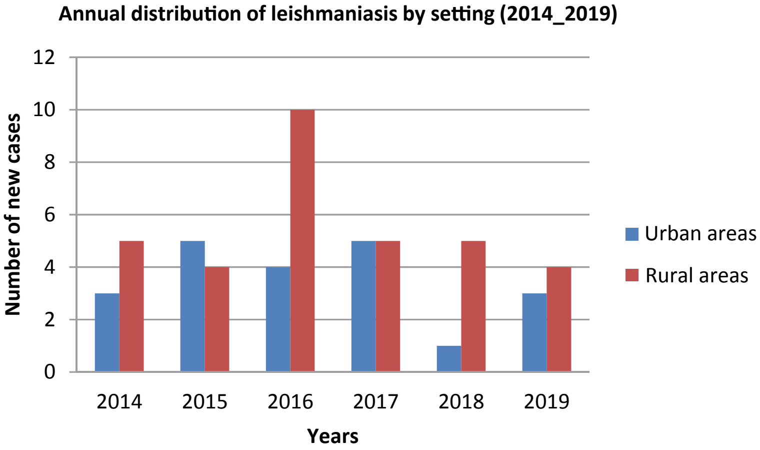


Fig. 2 Annual distribution of leishmaniasis by environment

From this figure, we can see that the year 2016 saw a high number of new cases of leishmaniasis, reaching 10 cases in rural areas, we also noticed that there is a dominance of leishmaniasis in rural areas compared to urban areas, with the exception of the years 2015 and 2017.

After 2016, we observe a regression in the number of new cases of leishmaniasis, especially in 2018 and 2019, which can be explained by the application of the Ministry of Health's programme to combat leishmaniasis and by the awareness of the local population [9].

The increase in new cases, especially in rural areas, is due to the appearance and the favourable spread of environment to the development and multiplication of vectors, particularly sandflies.

In some cases, people from rural areas move to urban areas and bring domestic animals with them, and may even raise livestock locally, providing suitable environments for the multiplication of *leishmania vector* sandflies.

These results are somewhat similar to the study of authors such as [10–12], who showed that this form of disease has appeared in some peri-urban and urban stations.

3.2 Study of the Spatial and Temporal Dynamics of Cutaneous Leishmaniasis Cases

Distribution of Cutaneous Leishmaniasis Cases According to Environment
Figure 3 shows the distribution of cutaneous leishmaniasis cases by type of medium.

According to the diagnostic analysis of this figure, we observed that cutaneous leishmaniasis is relatively more abundant in rural areas with a value of 58.14% against 41.86% in urban areas.

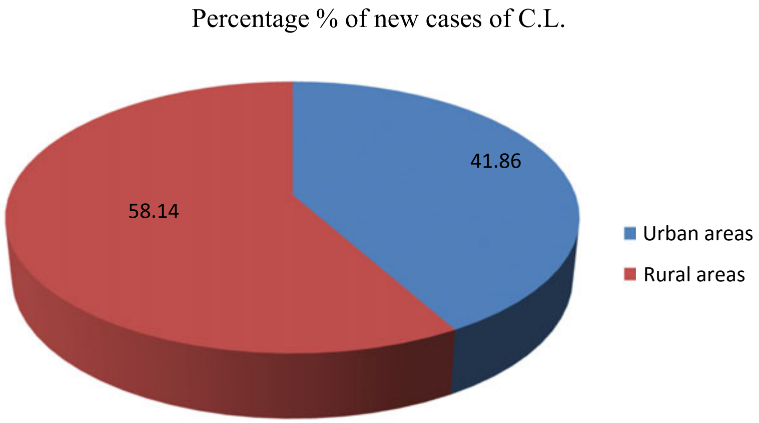


Fig. 3 Distribution of cutaneous leishmaniasis cases by setting

The analysis of the distribution of cutaneous leishmaniasis cases according to environment shows that there are factors that lead to the appearance of new cases of leishmaniasis in rural areas, for example the increase in population and unhealthy habitats where hygiene conditions are rudimentary.

These factors are already considered by Dr. Philippe Desjeux (Head of Trypanosomiasis and Leishmaniasis Control Programmes, Division of Tropical Disease Control WHO-Geneva) as risk factors [13].

Distribution of Cutaneous Leishmaniasis Cases According to Commune

The following figure presents the distribution of cutaneous leishmaniasis cases by commune during the 2014–2019 study period.

Following the diagnostic analysis of Fig. 4 representing the distribution of cases of cutaneous leishmaniasis by commune in the region of Meknes, we observed during the study period that the commune most affected by cutaneous leishmaniasis is CU Meknes, followed successively by CU Ouisslane, Mehaya and Ain karma, on the other hand, other communes did not record any case of cutaneous leishmaniasis, namely, Dar Oum Sultane, Sidi Slimane and Oued Jdida. On the other hand, we noticed that most of the communes were affected by cutaneous leishmaniasis with figures varying from one commune to another in 2016, knowing that the number of recorded cases does not exceed 6 cases in all communes except Meknes.

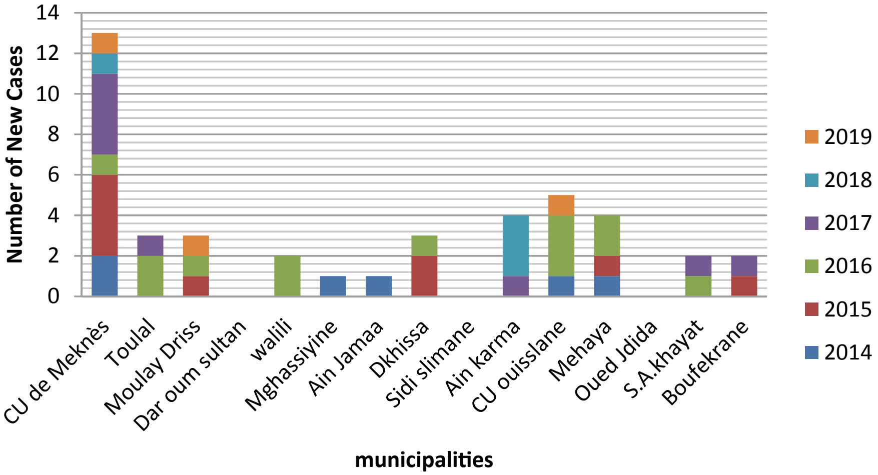


Fig. 4 Distribution of cutaneous leishmaniasis cases by commune

3.3 *Spatial and Temporal Study of Visceral Leishmaniasis Cases*

Figures 5 and 6 shows the spatial and temporal distribution of visceral leishmaniasis, during the period 2014–2019, by setting and by commune.

Distribution of the Incidence of Visceral Leishmaniasis by Environment
According to Fig. 5, we have noticed that there is a clear dominance of visceral leishmaniasis in the rural area with a value of 72.73% against 27.27% in the urban area.

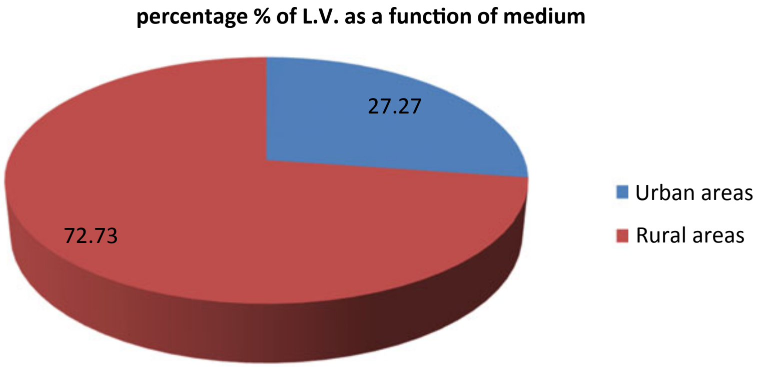


Fig. 5 Distribution of visceral leishmaniasis according to environment

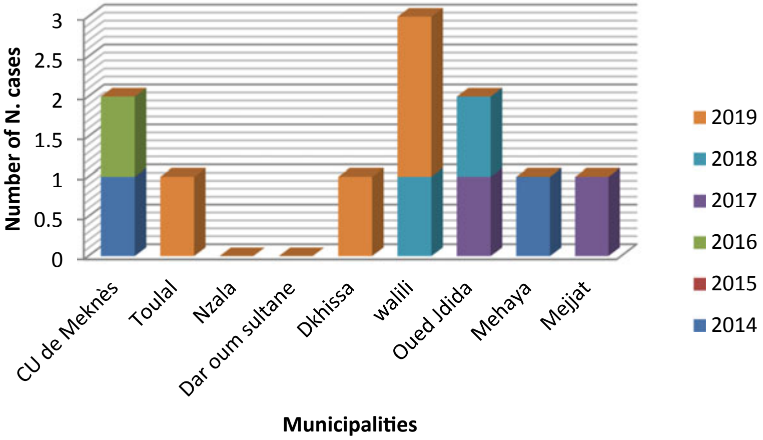


Fig. 6 Distribution of visceral leishmaniasis incidence by commune

These results could be explained by the increase in the number of inhabitants and the emergence of insalubrious places with poor hygienic conditions that favour the development of sandflies responsible for visceral leishmaniasis.

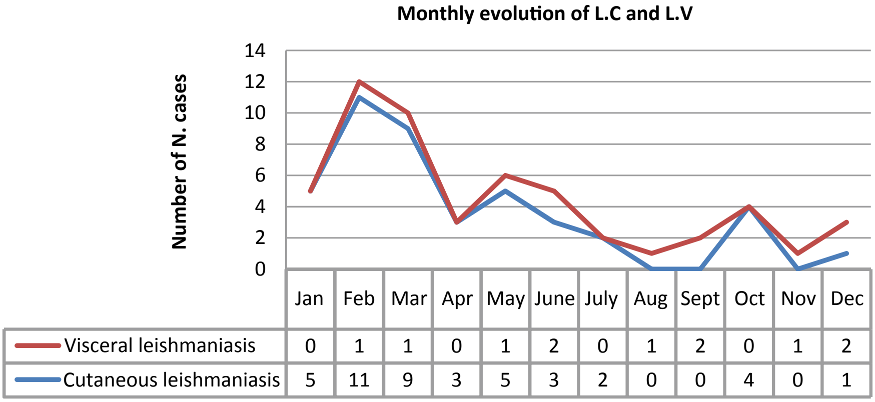
Distribution of the Incidence of Visceral Leishmaniasis by Commune
The analysis of the above figure shows that the number of new cases of visceral leishmaniasis was recorded with a maximum value of 3 in the commune of Walili, knowing that this value was taken in 2018 and 2019, followed by the communes of Meknes and Oued Jdida with the same value of 1.9. As for Nezala and Dar Oum sultane, the incidence rate of visceral leishmaniasis was zero.

3.4 Monthly Evolution of Cutaneous and Visceral Leishmaniasis Cases (2014–2019)

According to the epidemiological diagnostic results during the study period, as shown in Fig. 7, we see a very noticeable peak of visceral and cutaneous leishmaniasis in February with a maximum number of new cases recorded of 12, followed by two peaks that have decreased significantly, the first peak has a value of 6 in May and the second peak has a value of 4 in October.

We also note that there is an absence of cutaneous leishmaniasis in August, September and November, against 4 cases of visceral leishmaniasis, and an absence of visceral leishmaniasis in 4 different months; January, March, July and October, against 14 cases of cutaneous leishmaniasis.

In addition, the general pattern of cutaneous and visceral leishmaniasis curves shows simultaneous and fluctuating variations during the study period, which could be explained by the coexistence of *leishmania* vector sandflies or conditions favouring



	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
Visceral leishmaniasis	0	1	1	0	1	2	0	1	2	0	1	2
Cutaneous leishmaniasis	5	11	9	3	5	3	2	0	0	4	0	1

Fig. 7 Monthly evolution of cutaneous and visceral leishmaniasis from 2014 to 2019

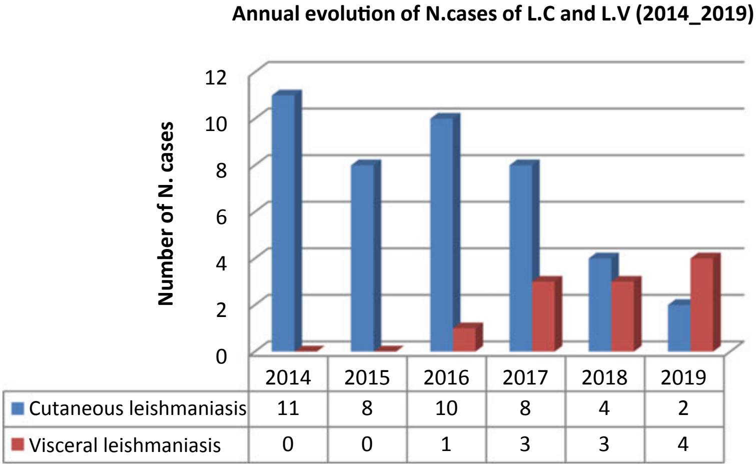
their development such as the wealth of stables and uncontrolled dumps produced by local inhabitants [9].

3.5 Annual Evolution of New Cases of C.L and V.L (2014–2019)

Figure 8 shows the annual evolution of new cases of cutaneous and visceral leishmaniasis during the study period from 2014 to 2019.

According to this figure, we observe a progressive decrease in the number of new cases of cutaneous leishmaniasis, whilst we notice a slight increase in visceral leishmaniasis which reaches the value of 4 in 2019, knowing that the years 2014 and 2015 did not record any new cases of visceral leishmaniasis.

These observations could be explained by the adoption of an approach to control leishmaniasis in general, by acting on the *leishmania* vectors and their reservoirs. But we can explain the increase in visceral leishmaniasis via the appearance of new species of *leishmania* responsible for visceral leishmaniasis and the settlement of *leishmania* carriers who have come from endemic regions.



	2014	2015	2016	2017	2018	2019
🟦 Cutaneous leishmaniasis	11	8	10	8	4	2
🟥 Visceral leishmaniasis	0	0	1	3	3	4

Fig. 8 Annual evolution of new cases of C.L. and V.L. (2014–2019)

3.6 Distribution of New Leishmaniasis Cases According to Age, Sex and Type of Leishmaniasis

Analysis of the distribution of new cases of leishmaniasis according to age, sex and type of leishmaniasis (Table 1) shows that this parasitosis mainly affects the age categories [0–19 years] and [60 years—over], which represented 66.66% and 12.96%, respectively.

In the population of the region of Meknes, infestation by the cutaneous form is predominant compared to the visceral form. Thus, we have noticed that cutaneous and visceral leishmaniasis are frequent in females with a percentage of 53.70% against 46.28% in males, knowing that infestation by the visceral form is present only in the age category [0–9 years] with a percentage of 20.37%.

3.7 Classification of Cases of Cutaneous and Visceral Leishmaniasis According to Their Origin

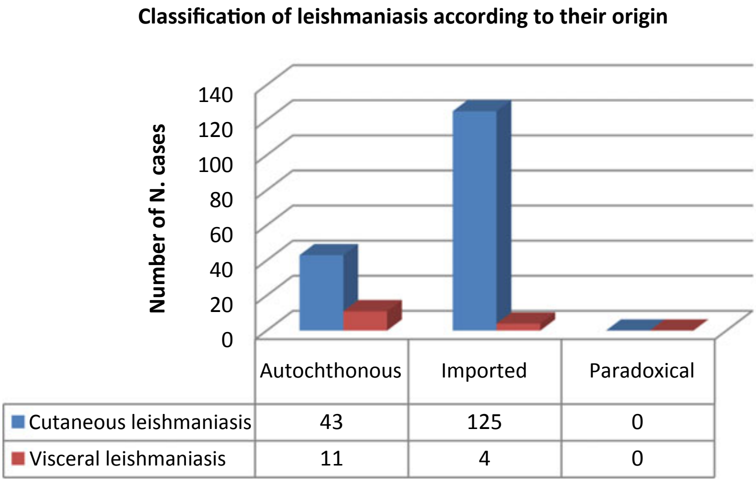
This Fig. 9 shows that there are three origins of leishmaniasis (autochthonous, imported or paradoxical) during the study period in the Meknes region.

We note a high number of new cases for the imported type which reaches 125 cases of cutaneous leishmaniasis against 43 new cases for the autochthonous type, knowing that there are a few people infected by visceral leishmaniasis for both the autochthonous and imported types, whilst we note an absence of leishmaniasis for the paradoxical type.

These results can be explained by the influence of neighbouring endemic regions, directly or indirectly, on the number of new cases of leishmaniasis via the movement of inhabitants during the year either during holidays or during their development of endemic areas, for example sidi Kacem, Moulay Yaakoub, Taounate and Hajeb.

Table 1 Distribution of new leishmaniasis cases according to age, sex and type of leishmaniasis

Type		Age															
		Total Nb.N.cases		Child [0–9]		Child [10–19]		Adult [20–29]		Adult [30–39]		Adult [40–49]		Adult [50–59]		Older [60 and Over]	
		N = 54	(100%)	N = 29	(53.70%)	N = 7	(12.96%)	N = 3	(5.55%)	N = 4	(7.40%)	*N* = 4	(5.55%)	N = 1	(1.85%)	N = 7	(12.96%)
Cutaneous leishmaniasis (C.L.)	Male	21	38.88	18	33.33	7	12.96	3	5.55	4	7.40	3	5.55	1	1.85	7	12.96
	Female	22	40.74														
Visceral leishmaniasis (VL)	Male	4	7.40	11	20.37	0		0		0		0		0		0	
	Female	7	21.96														



	Autochthonous	Imported	Paradoxical
🟦 Cutaneous leishmaniasis	43	125	0
🟥 Visceral leishmaniasis	11	4	0

Fig. 9 Classification of cutaneous and visceral leishmaniasis cases according to their origin

4 Conclusion

At the end of this retrospective study concerning all indigenous and imported cases detected during the period 2014–2019, we conclude that cutaneous and visceral leishmaniasis constitute a public health problem in south-central Morocco.

Cutaneous leishmaniasis affects all age groups in the majority of sectors and communes with a predominance of rural areas, whilst visceral leishmaniasis only infects children under the age of 9. It is also important to note that datas collected between 2014 and 2019 are not exhaustive and do not reflect the exact epidemiological situation of this parasitosis since most of the affected patients wait for spontaneous recovery and use traditional practices for the care and treatment of skin and visceral lesions.

Indeed, efforts to combat this disease are still insufficient, hence the need to improve awareness and information campaigns for the local population at risk and to encourage and monitor scientific studies in this field, such as entomological, mammalogical and molecular biology studies.

References

1. Dedet JP (2001) Répartition géographique des leishmanioses. Med Mal Infect 31:178–183. https://doi.org/10.1016/S0399-077X(01)80057-3
2. Pilly E, Collège des universitaires de maladies infectieuses et tropicales (France) (2015) Maladies infectieuses et tropicales. Alinéa Plus, Paris
3. Gutiérrez-Rebolledo GA, Drier-Jonas S, Jiménez-Arellanes MA (2017) Natural compounds and extracts from Mexican medicinal plants with anti leishmaniasis activity: an update. Asian

Pac J Trop Med 10(12):1105–1110. https://doi.org/10.1016/j.apjtm.2017.10.016

4. Tiwari N, Kishore D, Bajpai S, Singh R (2018) Visceral leishmaniasis: an immunological viewpoint on asymptomatic infections and post kala azar dermal leishmaniasis. Asian Pac J Trop Med 11(2):98. https://doi.org/10.4103/1995-7645.225016
5. El Alami Sanae (2009) 85 années de leishmaniose au Maroc. Université Mohamed V de Rabat. Faculté de Médecine et de Pharmacie
6. Houti L, Belgat S, Ikhlef-Allal A, Makhlouf B, Hamedi M, Rahou A, Bounoua L (2016) Impact du climat sur le développement de la leishmaniose cutanée dans la zone humide du Chott Ech Chergui, 17
7. Boussaa S, Boumezzough A (2014) Identification et caractérisation des gîtes larvaires de phlébotomes (Diptera: Psychodidae) à Marrakech (Maroc), 9
8. Haut-Commissariat au Plan. https://www.hcp.ma/region-meknes/RGPH-en-cartes_a106.html. https://www.hcp.ma/region-meknes/Monographie-de-la-Prefecture-deMeknes_a135.html
9. El Omari H, Chahlaoui A, Bouzid J, El Ouali Lalami AEO (2016) [Incidence of Cutaneous leishmaniasis in Meknes prefecture (centre of Morocco): a retrospective study of 56 cases collected between 2009 and 2013]. 18(1):9
10. Guernaoui S, Boumezzough A, Pesson B, et Pichon G (2005a) Entomological investigations in Chichaoua: an emerging epidemic focus of cutaneous leishmaniasis in Morocco. J Med Entomol 42:697–701
11. Rhajaoui M, Fellah H, Pratlong F, Dedet JP, Lyagoubi Leishmaniasis M (2004) due to Leishmania tropica MON-102 in a new Moroccan focus. Trans R Soc Trop Med Hyg 299–301
12. Arroub H, Belmekki M, Bencharki B, Habbari K (2016)Répartition spatio-temporelle de la leishmaniose cutanée dans les zones semi-arides Marocaines. Int J Innov Appl Stud 14(187–197)
13. Desjeux P (1999) Les leishmanioses. Aspect de santé publique et lutte. Edition Ellipses, 253 p

A Novel Context-Aware Recommendation Approach Based on Tensor Decomposition

Francesco Colace, Dajana Conte, Brij Gupta, Domenico Santaniello, Alfredo Troiano, and Carmine Valentino

Abstract In the information age, the ability to analyze data has a fundamental role. In this field, recommender systems, that are able to provide suggests to users analyzing the information provided to system, play a central role. Moreover, the use of contextual information make recommender systems more reliable. This paper aims to describe a novel approach for context-aware recommender systems that exploits the tensor decomposition CANDECOMP properties in order to provide ratings forecasts. The proposed approach is tested on DePaulMovie dataset in order to evaluate its accuracy, and the numerical results are promising.

Keywords Recommender systems · Context · CANDECOMP · Singular value decomposition

F. Colace (✉) · D. Santaniello
DIIN University of Salerno, Fisciano, Italy
e-mail: fcolace@unisa.it

D. Santaniello
e-mail: dsantaniello@unisa.it

D. Conte
DIPMAT University of Salerno, Fisciano, Italy
e-mail: dajconte@unisa.it

B. Gupta
International Center for AI and Cyber Security Research and Innovations, Asia University, Taichung 413, Taiwan

A. Troiano
NetCom Group, Napoli, Italy
e-mail: a.troiano@netcomgroup.eu

C. Valentino
DIPMAT University of Salerno, Fisciano, Italy
e-mail: cvalentino@unisa.it

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_39

1 Introduction

In the big data [14] era, the ability to select information is fundamental. This achievement is not simple among all data available for a system. Indeed, the number of collected data is enormous. In this field, one of the most important tools able to support users is recommender system (RS) [7, 11, 13].

Recommender systems (RSs) are information filtering tools that give support to users in order to select among all available items [25]. They are able to select the right information about users preferences and items features in order to provide an estimation that allows to classify items between useful or not for users.

The elements of RSs are users of the system, items that have to be suggested and transaction [25], that represent the interaction between a user and the system. The most common transaction form is rating, an implicit or explicit evaluation of the user preference about an item [25]. Moreover, rating can be seen as a function that has as domain the Cartesian product of users set U and items set I.

$$r : (u, i) \in U \times I \mapsto r(u, i) \in \mathcal{R} \tag{1}$$

The principal problem of RSs is to determinate $r_{ui} = r(u, i)\ \forall (u, i) \in U \times I$. The mode to achieve rating forecast enables to classify RSs based on the different strategies.

The most common recommendation strategies are content-based, collaborative filtering and hybrid [6].

Content-based RSs [12, 23] are based on the creation of users and items profiles. These profiles are exploited in order to obtain user-item affinity. The most common form exploited to calculate user-item affinity is cosine similarity [17].

Collaborative filtering RSs [31] are based on known ratings provided by users and can be divided in two different classes: memory-based and model-based. Memory-based ones aim to divide users (user-based) or items (item-based) into groups [24]. Model-based ones aim to create a numerical model of the problem through the factorization of ratings matrix [25].

Hybrid RSs exploits the principal features of the previous methods in order to overcome the problems of the single method [10].

The development of RSs brought to the introduction of new elements in order to improve provided rating forecasts. Context [2, 16] is one of these elements and allows to obtain context-aware recommender systems [9]. The awareness of context is exploited in order to obtain more appropriate rating forecasts.

Context can be defined as "any information useful to characterize the situation of an entity that can affect the way users interact with systems" [1, 30] and allows to define a new rating function that has as domain the Cartesian product of users set U, items set I and the contextual sets $C_1, \ldots, C_n$ that contain the contextual information analyzed by the system.

$$r : U \times I \times C_1 \times \cdots \times C_n \mapsto \mathcal{R} \tag{2}$$

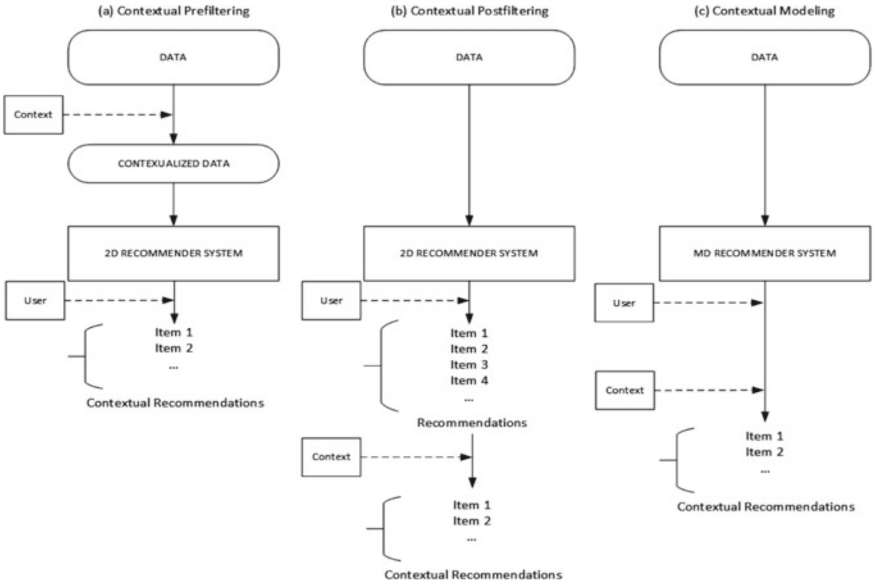


Fig. 1 Strategies for introducing contextual information into a recommender system [2]

The introduction of context in a recommender system is possible through three different strategies [2, 10]:

- Contextual Pre-Filtering: the contextual information is analyzed before the recommendation phase in order to select the proper elements to provide to recommender system;
- Contextual Post-Filtering: the contextual information is exploited in order to select the proper rating forecasts provided by the recommendation phase;
- Contextual Modeling: contextual information are exploited in the recommendation phase in order to generate appropriate rating forecasts.

Figure 1 presents a summary of the described strategies.

The aim of this paper is the description of a novel context-aware recommendation approach. The paper is organized as follows: Sect. 2 contains background and related works; in Sect. 3 the proposed approach is described, Sect. 4 presents the experimental phase exploited to evaluate the method described in Section 3; in Sect. 5 there are conclusions and future works.

2 Background and Related Works

In the recommender systems field, there is a great variety of strategies that are exploited in order to obtain rating forecasts.

Content-based methods can exploit term frequency and inverse document frequency in order to create profiles [22, 28]. Another technique exploited in content-based recommendation is Latent Dirichlet Allocation [28].

In memory-based recommendation, the clustering of users or items can be obtained through Pearson correlation [18] or through K-nearest neighbors algorithm [29]. In model-based recommendation, there are various factorization methods exploited such as probabilistic matrix factorization (PMF), non-negative matrix factorization (NMF) and singular value decomposition (SVD) [8]. In particular, singular value decomposition allows to factorize the ratings matrix $R \in \mathbb{R}^{m \times n}$ that refers to a system of m users and n items, in the product of three matrices: the matrices $U \in \mathbb{R}^{m \times m}$ and $V \in \mathbb{R}^{n \times n}$ defined matrices of left and right singular vectors, and the matrix $D = \mathrm{diag}\left(\sigma_1, \ldots, \sigma_p\right) \in \mathbb{R}^{m \times n}$ defined matrix of the singular values, where $p = \min\{m, n\}$.

$$R = UDV^{\mathrm{T}} \tag{3}$$

Fixed the value $k \in \mathbb{N} : k \leq p$, the Eckart-Young Theorem [12] allows to approximate the rating matrix through the matrices $U_k \in \mathbb{R}^{m \times k}$ obtained from U, $V_k \in \mathbb{R}^{n \times k}$ obtained from V, and $D_k \in \mathbb{R}^{k \times k}$ obtained from D.

$$R \approx U_k D_k V_k^T \tag{4}$$

The Eckart-Young Theorem guarantees that the matrix $R_k = U_k D_k V_k^T$ is the matrix of rank k that best approximates the ratings matrix R [12].

Matrix factorization is also exploited by context-aware RSs. Indeed, Baltrunas et al. [4] developed context-aware matrix factorization (CAMF), a contextual modeling method that support the matrix factorization with bias related to contextual information. Instead, splitting approaches [10, 32] are pre-filtering methods that select the proper row or columns of the ratings matrix and generate rating forecasts through the matrix factorization. These approaches divide the known rating in the specific context. Thus, there are more rows of rating matrix referred to the user $u \in U$ (user splitting) or more columns of rating matrix referred to the item $i \in I$ (item splitting) on the basis of the contextual information.

The Tensor factorization [21] is also exploited by context-aware RSs. Karatzoglou et al. [20] exploit high-order singular value decomposition (HOSVD) [3] in order to generate rating forecasts through a machine learning algorithm. Instead, Chen et al. [15] propose a multi-criteria recommender system that exploits stacked denoising autoencoder and CANDECOMP. In particular, canonical decomposition (CANDECOMP) allows to factorize tensor $\mathcal{R} \in \mathbb{R}^{m \times n \times l}$ through the sum of s rank-1 tensors [21]:

$$\mathcal{R}_{ijz} = \sum_{h=1}^{s} \lambda_h A_{ih} B_{jh} C_{zh} \tag{5}$$

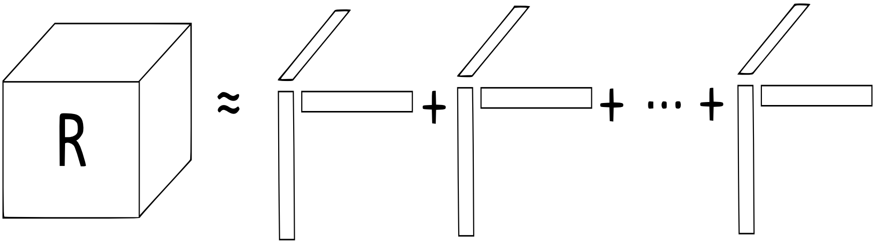


Fig. 2 Graphical representation of CANDECOMP [21]

where $A \in \mathbb{R}^{m\times s}$, $B \in \mathbb{R}^{n\times s}$ and $C \in \mathbb{R}^{l\times s}$ are matrices with columns of unitary norm and $\lambda = (\lambda_1, \ldots, \lambda_s) \in \mathbb{R}^s$ (Fig. 2).

The CANDECOMP is exploited in Sect. 3 in order to describe a novel approach for Context-Aware Recommender Systems.

3 The Proposed Approach

In this section, the proposed approach is described. It consists of an heuristic method that exploits CANDECOMP and SVD properties in order to generate rating forecasts.

The system is supposed to have m users, n items and one contextual dimension that can assume l values. Thus, the ratings tensor $\mathcal{R} \in \mathbb{R}^{m\times n\times l}$ has three dimensions. Instead, the matrix $R \in \mathbb{R}^{m\times n}$ contains the ratings without context and can be given by dataset. If the dataset does not provide known ratings without context, they can be calculated through the average of all l contextual domains.

Firstly, the singular value decomposition role is evaluated. The relation (4) allows to approximate the known rating. Indeed, the product of matrices $P = U_k\sqrt{D_k} \in \mathbb{R}^{m\times k}$ and $Q = V_k\sqrt{D_k} \in \mathbb{R}^{n\times k}$ approximates the rating matrix:

$$R \approx PQ^T \tag{6}$$

The relation (6) is made explicit trough the relation (7) where $p_{ih} = (U_k)_{ih}\sqrt{\sigma_h}$ and $q_{jh} = (V_k)_{jh}\sqrt{\sigma_h}$.

$$r_{ij} \approx \sum_{h=1}^{k} \sigma_h \, (U_k)_{ih} \, (V_k)_{hj} = \sum_{h=1}^{k} p_{ih} q_{jh} \tag{7}$$

P and Q are matrices that create fake numerical profiles of users and items, respectively. The objective of the proposed approach is the construction of ratings forecasts through the calculation of the fake numerical profile of the l contextual dimensions. In order to achieve this purpose, the contextual dimension $z \in \{1, \ldots, l\}$ is fixed, and the following hypothesis are done:

- the values k of relation (4) and s of relation (5) coincide;
- the matrix A of relation (5) is equal to U_k of relation (6);
- the matrix B of relation (5) is equal to V_K of relation (6).
- The relation $\lambda_h = \sigma_h \times \gamma_h \ h = 1, \ldots, k$ is supposed valid, where $\gamma_h > 0 \ h = 1, \ldots, k$

The done hypothesis can be integrated in the relation (5).

$$\mathcal{R}_{ijz} = \sum_{h=1}^{k} \lambda_h A_{ih} B_{jh} C_{zh} = \sum_{h=1}^{k} \sigma_h \gamma_h \left(U_k\right)_{ih} \left(V_k\right)_{jh} C_{zh} \tag{8}$$

The matrix $W \in \mathbb{R}^{l \times k}$ has the elements $W_{zh} = \gamma_h C_{zh} \ \ h = 1, \ldots, k \ z = 1, \ldots, l$. Thus, the previous relation can be reformulated as follows:

$$\mathcal{R}_{ijz} = \sum_{h=1}^{k} P_{ih} Q_{jh} W_{zh} \tag{9}$$

Let the element $t \in \{1, \ldots, k\}$ fixed, the weighted average on items can be done as follows:

$$\frac{\sum_{j=1}^{n} \left(V_k\right)_{jt} \mathcal{R}_{ijz}}{\sum_{j=1}^{n} \left|\left(V_k\right)_{jt}\right|} = \sum_{h=1}^{k} \frac{\sum_{j=1}^{n} \left(V_k\right)_{jt} P_{ih} Q_{jh}}{\sum_{j=1}^{n} \left|\left(V_k\right)_{jt}\right|} W_{zh} \tag{10}$$

Thus, the weighted average on users can be done:

$$\frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left(U_k\right)_{it} \left(V_k\right)_{jt} \mathcal{R}_{ijz}}{\left(\sum_{i=1}^{m} \left|\left(U_k\right)_{it}\right|\right) \left(\sum_{j=1}^{n} \left|\left(V_k\right)_{jt}\right|\right)} = \sum_{h=1}^{k} \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left(U_k\right)_{it} \left(V_k\right)_{jt} P_{ih} Q_{jh}}{\left(\sum_{i=1}^{m} \left|\left(U_k\right)_{it}\right|\right) \left(\sum_{j=1}^{n} \left|\left(V_k\right)_{jt}\right|\right)} W_{zh} \tag{11}$$

In order to simplify the relation (11), the following quantities are defined:

$$\bar{\mathcal{R}}_t^{(z)} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left(U_k\right)_{it} \left(V_k\right)_{jt} \mathcal{R}_{ijz}}{\left(\sum_{i=1}^{m} \left|\left(U_k\right)_{it}\right|\right) \left(\sum_{j=1}^{n} \left|\left(V_k\right)_{jt}\right|\right)} \quad t = 1, \ldots, k \tag{12}$$

$$\alpha_{th}^{(z)} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left(U_k\right)_{it} \left(V_k\right)_{jt} P_{ih} Q_{jh}}{\left(\sum_{i=1}^{m} \left|\left(U_k\right)_{it}\right|\right) \left(\sum_{j=1}^{n} \left|\left(V_k\right)_{jt}\right|\right)} \quad t, h = 1, \ldots, k \tag{13}$$

The relations (12) and (13) allow to reformulate the relation (11) as follows:

$$\bar{\mathcal{R}}_t^{(z)} = \sum_{h=1}^{k} \alpha_{th}^{(z)} W_{zh} \quad t = 1, \ldots, k \tag{14}$$

The relation (14) consists of a linear system that allows to determinate the fake numerical profile $(W_{z1}, \ldots, W_{zk})$ of the context dimension z. The resolution of all the l linear systems allows to identify the elements of the matrix $W \in \mathbb{R}^{l \times k}$.

In the operative phase, the averages calculated are done on the known ratings in the system.

Finally, in order to improve the rating forecasts, contextual bias are exploited. Indeed, the rating forecasts are calculated as follows:

$$\hat{\mathcal{R}}_{ijz} = \bar{r}_z + b_{iz} + b_{jz} + \sum_{h=1}^{k} P_{ih} Q_{jh} W_{zh} \tag{15}$$

where $\bar{r}_z$ is the average of all known ratings in the context z, b_{iz} is the user i bias in the context z, b_{jz} is the item j bias in the context z and $\sum_{h=1}^{k} P_{ih} Q_{jh} W_{zh}$ is seen as the affinity of user i and item j in the context z.

The principal advantage of the proposed approach is the possibility to calculate the context profiles in order to support the collaborative filtering recommendation method with a content-based one. Indeed, a hybrid recommendation method can be developed through a proper initialization of users and items profiles. The disadvantage of the proposed method is the need of known rating in order to calculate the context profiles.

4 Experimental Phase

In this section, the experimental phase is described. The numerical results are obtained through the dataset DePaulMovie [19, 33] that contains 5043 known ratings collected on 97 users, 79 items and 3 context dimensions. The 5043 ratings are divided in 1448 ratings without context and 3595 contextual ratings.

The contextual information exploited by the dataset are location that can assume the values home and cinema, companion that can assume the values alone, family and friends, and time that can assume the values weekend and weekday. Since the proposed approach is defined on one contextual dimension, the three contextual domain of DePaulMovie are taken into account as shown in Table 1. Indeed, the value of l is 12, the value of m is 97 and the value of n is 79.

The aim of the experimental phase is the evaluation of the proposed approach accuracy. In order to achieve this aim, mean absolute error (MAE) and root mean squared error (RMSE) are calculated according to the following formulas:

$$\text{MAE} = \frac{1}{|D|} \sum_{\mathcal{R}_{ijz} \in D} \left| \mathcal{R}_{ijz} - \hat{\mathcal{R}}_{ijz} \right| \tag{16}$$

$$\text{RMSE} = \sqrt{\frac{1}{|D|} \sum_{\mathcal{R}_{ijz} \in D} \left(\mathcal{R}_{ijz} - \hat{\mathcal{R}}_{ijz} \right)^2} \tag{17}$$

Table 1 Values that context can assume in the proposed approach

	Contexts
1	(Home, alone, weekend)
2	(Home, alone, weekday)
3	(Home, family, weekend)
4	(Home, family, weekday)
5	(Home, friends, weekend)
6	(Home, friends, weekday)
7	(Cinema, alone, weekend)
8	(Cinema, alone, weekday)
9	(Cinema, family, weekend)
10	(Cinema, family, weekday)
11	(Cinema, friends, weekend)
12	(Cinema, friends, weekday)

Table 2 Numerical results on DePaulMovie dataset

	MAE	RMSE
CAMF-CI [4]	0.7122	0.9660
CAMF-CU [4]	0.6682	0.9198
CAMF-C [4]	0.7029	0.9571
CAMF-CUCI [4, 33]	0.6753	0.9206
Item splitting [5]	0.7185	1.0362
User splitting [27, 34]	0.7361	1.0588
The proposed approach	0.6591	0.9186

where D is the dataset that contains the contextual ratings, $\mathcal{R}_{ijz}$ is the known rating in the dataset D and $\hat{\mathcal{R}}_{ijz}$ is the rating forecast provided by the context-aware recommender system. Moreover, the cross-validation fivefold [26] technique is exploited.

The results of the comparison methods are taken from CarsKit [33]. In Table 2 the numerical results are presented.

Table 2 proves that the proposed approach returns better results than the comparison methods.

5 Conclusions and Future Works

In this paper, a focus on recommender systems and context-aware recommender systems is done. In particular, the singular value decomposition and CANDECOMP are presented in Sect. 2, and they are exploited in Sect. 3 in order to present an heuristic context-aware recommender system. Finally, the numerical results are shown in Sect. 4. The experimental phase evidences that the proposed approach return better results than the comparison methods.

In order to improve the proposed approach, some improvements can be exploited. Since all items and users has the some contextual profile, a neighbor method will be exploited in order to divide items that improve their ratings in the contextual dimension and items that get worse their ratings in the contextual dimension. Moreover, others dataset is going to be exploited in order to confirm the goodness of the proposed approach.

Finally, a proper method in order to create users and items profiles is going to be developed in order to obtain an hybrid approach that enables the system to overcome the cold star problem related to lack of known ratings.

References

1. Abowd GD, Dey AK, Brown PJ, Davies N, Smith M, Steggles P (1999) Towards a better understanding of context and context-awareness. In: International symposium on handheld and ubiquitous computing. Springer, pp 304–307
2. Adomavicius G, Tuzhilin A (2011) Context-aware recommender systems. In: Recommender systems handbook. Springer, pp 217–253
3. Ballester-Ripoll R, Lindstrom P, Pajarola R (2019) Tthresh: tensor compression for multidimensional visual data. IEEE Trans Vis Comput Graph 26(9):2891–2903
4. Baltrunas L, Ludwig B, Ricci F (2011) Matrix factorization techniques for context aware recommendation. In: Proceedings of the fifth ACM conference on recommender systems, pp 301–304
5. Baltrunas L, Ricci F (2009) Context-based splitting of item ratings in collaborative filtering. In: Proceedings of the third ACM conference on recommender systems, pp 245–248
6. Batmaz Z, Yurekli A, Bilge A, Kaleli C (2019) A review on deep learning for recommender systems: challenges and remedies. Artif Intell Rev 52(1):1–37
7. Bobadilla J, Ortega F, Hernando A, Gutiérrez A (2013) Recommender systems survey. Knowl-Based Syst 46:109–132
8. Bokde D, Girase S, Mukhopadhyay D (2015) Matrix factorization model in collaborative filtering algorithms: a survey. Procedia Comput Sci 49:136–146
9. Carbone M, Colace F, Lombardi M, Marongiu F, Santaniello D, Valentino C (2021) An adaptive learning path builder based on a context aware recommender system. In: 2021 IEEE frontiers in education conference (FIE). IEEE, pp 1–5
10. Casillo M, Colace F, Conte D, Lombardi M, Santaniello D, Valentino C (2021) Context-aware recommender systems and cultural heritage: a survey. J Amb Intell Humanized Comput, pp 1–19
11. Casillo M, Colace F, De Santo M, Lombardi M, Mosca R, Santaniello D (2020) A recommender system for enhancing coastal tourism. In: The international research & innovation forum. Springer, pp 113–122
12. Casillo M, Conte D, Lombardi M, Santaniello D, Troiano A, Valentino C (2022) A content-based recommender system for hidden cultural heritage sites enhancing. In: Proceedings of sixth international congress on information and communication technology. Springer, pp 97–109

13. Casillo M, De Santo M, Lombardi M, Mosca R, Santaniello D, Valentino C (2021) Recommender systems and digital storytelling to enhance tourism experience in cultural heritage sites. In: 2021 IEEE international conference on smart computing (SMARTCOMP). IEEE, pp 323–328
14. Chen R, Hua Q, Chang Y-S, Wang B, Zhang L, Kong X (2018) A survey of collaborative filtering-based recommender systems: from traditional methods to hybrid methods based on social networks. IEEE Access 6:64301–64320
15. Chen Z, Gai S, Wang D (2019) Deep tensor factorization for multi-criteria recommender systems. In: 2019 IEEE international conference on big data (big data). IEEE, pp 1046–1051
16. Colace F, De Santo M, Lombardi M, Mosca R, Santaniello D (2020) A multilayer approach for recommending contextual learning paths. J Internet Serv Inf Secur 10(2):91–102
17. De Gemmis M, Lops P, Musto C, Narducci F, Semeraro G (2015) Semantics-aware content-based recommender systems. In: Recommender systems handbook. Springer, pp 119–159
18. Desrosiers C, Karypis G (2011) A comprehensive survey of neighborhood-based recommendation methods. Recommender systems handbook, pp 107–144
19. Ilarri S, Trillo-Lado R, Hermoso R (2018) Datasets for context-aware recommender systems: Current context and possible directions. In: 2018 IEEE 34th international conference on data engineering workshops (ICDEW). IEEE, pp 25–28
20. Karatzoglou A, Amatriain X, Baltrunas L, Oliver N (2010) Multiverse recommendation: n-dimensional tensor factorization for context-aware collaborative filtering. In: Proceedings of the fourth ACM conference on recommender systems, pp 79–86
21. Kolda TG, Bader BW (2009) Tensor decompositions and applications. SIAM Rev 51(3):455–500
22. Lops P, De Gemmis M, Semeraro G (2011) Content-based recommender systems: State of the art and trends. Recommender systems handbook, pages 73–105
23. Mohamed MH, Khafagy MH, Ibrahim MH (2019) Recommender systems challenges and solutions survey. In: 2019 international conference on innovative trends in computer engineering (ITCE), . IEEE, pp 149–155
24. Ning X, Desrosiers C, Karypis G (2015) A comprehensive survey of neighborhood-based recommendation methods. Recommender systems handbook, pp 37–76
25. Ricci F, Rokach L, Shapira B (2015) Recommender systems: introduction and challenges. In: Recommender systems handbook. Springer, pp 1–34
26. Rodriguez JD, Perez A, Lozano JA (2009) Sensitivity analysis of k-fold cross validation in prediction error estimation. IEEE Trans Pattern Anal Mach Intell 32(3):569–575
27. Said A, De Luca EW, Albayrak S (2011) Inferring contextual user profiles-improving recommender performance. In: Proceedings of the 3rd RecSys workshop on context-aware recommender systems
28. Somasundaram K, Murphy GC (2012) Automatic categorization of bug reports using latent dirichlet allocation. In: Proceedings of the 5th India software engineering conference, pp 125–130
29. Subramaniyaswamy V, Logesh R (2017) Adaptive KNN based recommender system through mining of user preferences. Wirel Person Commun 97(2):2229–2247
30. Villegas NM, Sánchez C, Díaz-Cely J, Tamura G (2018) Characterizing context-aware recommender systems: a systematic literature review. Knowledge-based systems 140:173–200
31. Wang X, He X, Wang M, Feng F, Chua T-S (2019) Neural graph collaborative filtering. In: Proceedings of the 42nd international ACM SIGIR conference on research and development in information retrieval, pp 165–174
32. Zheng Y, Burke R, Mobasher B (2014) Splitting approaches for context-aware recommendation: An empirical study. In: Proceedings of the 29th annual ACM symposium on applied computing, pp 274–279
33. Zheng Y, Mobasher B, Burke R (2015) Carskit: A java-based context-aware recommendation engine. In: 2015 IEEE international conference on data mining workshop (ICDMW). IEEE, pp 1668–1671
34. Zheng Y, Mobasher B, Burke RD (2013) The role of emotions in context-aware recommendation. Decisions@ RecSys, 21–28

Application of E-commerce Technologies in Accelerating the Success of SME Operation

Ziad Almtiri, Shah J. Miah, and Nasimul Noman

Abstract Application of electronic commerce (e-commerce) technologies has increased notably over the past two decades in different business sectors. In particular, the technologies of B2C operations have significantly improved the productivity of online small businesses such as SMEs. Systematic literature reviews in this domain categorized different, benefits but a limited number of studies on SME success from the view of information systems (IS) research exist, which needs to be taken for further attention. Through a comprehensive analysis, this study introduces a conceptual framework for the application of e-commerce technologies in accelerating SME operation. Content analysis methodology was adopted for generating the outcome associated with the success of the technologies in SMEs.

Keywords SMEs · B2C · Small business · Literature review · Success factors · Technology acceptance

1 Introduction

E-commerce technologies have proliferated over the past two decades for their growing applications. The applications are rapidly increasing in improving productivity and relevance in the online business sector [1]. E-commerce literature provides insights of various latest understanding of the effective operation of online businesses. Given that the business world is rapidly changing, it is crucial to understand the advantages matrix and different types of applications of e-commerce technologies

Z. Almtiri (✉)
Department of Management Information Systems, Taif University, Taif, Saudi Arabia
e-mail: ziad_almtiri@outlook.com

Z. Almtiri · S. J. Miah
Newcastle Business School, University of Newcastle, Callaghan, NSW, Australia
e-mail: shah.miah@newcastle.edu.au

N. Noman
School of Information and Physical Sciences, University of Newcastle, Callaghan, NSW, Australia
e-mail: nasimul.noman@newcastle.edu.au

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_40

and their appropriate meanings in terms of achieving business success, particularly for B2C businesses. Acknowledging this, in this paper we explore insights of the application of B2C e-commence technologies in Saudi Arabian context, so that new conceptual framework of e-commerce technologies application can be outlined that would ensure the success of business.

There are numerous literature review studies in e-commerce. According to Statista [2], 90% of individuals in Saudi Arabia have access to the Internet. The statistics also show that up to 80% of the population participates in online shopping. Grbovic et al. [3] examined the mandatory features advertising should have to promote e-commerce after executing information technology, considering that it is a primary tool used to boost the effectiveness of technology adoption. Hallikainen and Laukkanen [1] reviewed the influence of culture on conviction in e-commerce. Arguably, nationwide culture often unswervingly influences perceived trust. Alkhalil et al. [4] support the arguments by explaining that businesses in Saudi have identified the role of e-commerce in improving consumer trust since the technologies enhance the efficiency of the entities. Consumers in Saudi prefer to transact with entities that have effective online systems that promote their fast and effective service delivery.

2 Study Background

In the business world, technological advancements have impacted nearly every facet of the sector. Businesses have now adopted artificial intelligence, chatbots, and virtual assistants in the retail industry into their routine operations [5]. Although the reasons for adoption may vary from business to business, the primary motives are to help provide exceptional customer experience through instant communication, providing support without the need of data management and security, live employees, and more [6]. The primary e-commerce technologies already adopted by SME's often include electronic funds handover, record administration systems, computerized data collection schemes, Internet marketing, online transaction processing, and mobile transfer [7]. For instance, in Saudi Arabia, nearly all restaurants in have adopted an electronic payment system and POS system for making orders, recording sales, and printing reports for sales, employee performance, profits, fast-moving, among others. In 2020, debit cards were the most dominant payment method for online shopping in the Kingdom, comprising 60% of all transactions [7]. Overall, most e-commerce technologies such as electronic transfer of funds, Internet marketing, and digital inventory management systems have already been implemented by a significant number of SMEs in Saudi Arabia, and more growth is expected in the future [8].

The effects of e-commerce can be seen in various sectors of the Saudi economy. For instance, the revenue earned by SME's in the transport, hospitality, and food sector grew by nearly 50% in the past two years [7]. During the same duration, the government revenue attributed to these sectors grew by over 60% [7]. In a study to assess the adoption of e-commerce in the entertainment sector, Purwati [9] found that ease of payment, availability of electronic payment systems, and exceptional customer service by SMEs in Saudi's entertainment sector have facilitated the fast growth of cinemas and other entertainment joints (Table 1).

Table 1 Critical analysis of the previous studies of e-commerce

Journal articles	The current literature review assessed	Articulated research gaps for the current research
Export.gov [10]	Significant trends in e-commerce development insight into the state of it in the country and comparing it to other retailing technologies	Basis for determining key performance indicators (KPIs) in assessing the success of e-commerce implementation. Further analysis will also provide recommendations to SMEs in Riyadh when adopting technologies
Sacha Orloff [11]	Sixty-five percent of Saudi Arabia's population has access to the internet; online shoppers in the country have rapidly increased	We noted that one of the essential factors contributing to the development of e-commerce is the ease of use. The relationship between ease of use and the success of e-commerce will be explored
Grvobic et al. [3]	It examined the features of advertising needed to promote e-commerce after implementing information technology	Analyses of online advertising as one of the success factors in technology adoption. The study assesses how e-commerce enhances the efficiency of advertising on diverse online platforms
Hallikainen and Laukkanen [1]	They examined how culture influences trust in e-commerce. National culture can directly influence perceived trust	Ease of use will be used as one of the factors affecting the desire of consumers to use the service
Mazzarol [12]	Examining SMEs commitment to Electronic—commerce, business, and marketing	Connection between the comfort of expenditure and the accomplishment of E-commerce will be discovered
Xuhua et al. [6]	Explains effects of business-to-consumer e-commerce implementation on the economic advantage of manufacturing SMEs	Deliberate promotion as one of the success factors in technology implementation

2.1 Role of Technologies in E-commerce

While e-commerce has significantly simplified the customer buying experience, establishing an efficient e-commerce structure requires many tools and technologies combined to ensure the smooth performance of commercial transactions. Helal [13] described an investigation of the use of social media for e-commerce among Saudi small businesses and used a qualitative interpretive philosophical point of view. This study uses a multiple case study strategy. For Helal's research [13], four small businesses in Saudi Arabia were used and determined that traditional e-commerce currently has many obstacles that limit its distribution. Moreover, this study determined that social networks benefit small and medium enterprises in Saudi Arabia. The model she developed suggests a direct link between social capital, word of mouth, and trust in the context of small businesses in Saudi Arabia. Export.gov [10] argues that a customer relationship management tool creates exceptional customer experience on a company's website while tracking those experiences. Adopting such a customer relationship management system and a dedicated customer support team gives a business a competitive advantage relative to other firms without customer engagement [13]. In addition, companies have started adopting methods for providing a personalized customer experience. Such marketing activities help build a loyal customer base and thereby increasing sales and profits [4]. To stay competitive in the market, businesses follow newest trends. Among the current most popular technologies used by enterprises are social media platforms such as Instagram, Facebook, Twitter, and others.

3 Research Methodology

The study is based on a systematic literature review that is conducted to point out the scope and prospect for diverse applications of e-commerce technologies for online businesses. We survey the literature in academic journals, books, and conference articles, having the objectives of collecting, soring, and synthesize existing studies related to applications of e-commence technologies. The surveyed sample articles focused on several applications of e-commence technologies for SMEs. The findings are leading to develop a new framework to ensure success of SME operation. We searched several databases such as IEEE, Elsevier, Springer, Association for Computing Machinery (ACM), IEEE Xplore, and other IS journals. In searching, we have used various keywords such as: "e-business" and "Saudi", "e-commence" and "Saudi" OR "developing countries", "e-commerce technologies and SME" and "e-business technologies and SMEs", "Saudi and SMEs" and "business technologies and SMEs".

Under this approach, we set two main objectives for the SLR study: gathering insights into diversified submissions of e-commerce skills and critical issues. In Saudi Arabia, the primary e-commerce technologies already adopted by SME's include electronic funds transfer, record running systems, automatic statistics collection structures, Internet marketing, online transaction processing, and mobile transfer.

This study adopts content analysis methodology to generate the outcome linked to the success of technologies in SMEs. Creswell [14] defines content analysis methodology as a technique incorporated to make valid and replicate references by coding and interpreting textual material. Overall, this study reviews relevant literature on B2C e-commerce for developing a new conceptual application framework of e-commerce technologies that facilitate the success of SMEs. Firstly, various studies addressing the meaning, implications, and benefits of e-commerce technologies on business are analyzed. This involves exploring varying options and functions of e-commerce technologies which are among the primary factors to transformational goals. Considering that a website is a primary tool in e-commerce, numerous studies highlight the features one should have. With such a website, unnecessary complexities that may hinder fast and efficient shopping.

4 Findings Leading to a Conceptual Framework

Notably, the business environment has widely accepted e-commerce enabling firms to promote their products and services for better results. With this growth, online commercial fields are rapidly growing, with a considerable number of traditional markets evolving to online platforms. Similarly, the growing electronic devices adoption among people has made B2C retail more pertinent. Thus, considering that e-commerce requires electronic devices to make its application more effective, and the use of such devices is on the rise, its implementation by SMEs has more significant potential.

User-generated reviews can boost its market share and sales through advertising for a company offering high-quality commodities and services. In a study to evaluate the impact of user ratings on websites, Gregory et al. [15] found that 53% of customers prefer buying from a company rated five stars and above. While e-commerce has meaningfully abridged the client's buying experience, inaugurating a well-organized e-commerce structure necessitates many tools and skills shared to ensure the smooth performance of commercial transactions (Table 2).

The concept behind this project is to employ the Retail Merchant Associations (RMA). Even if the user doesn't have a standard PC or Internet connection, the RMA will assist in selling over the Internet. The RMA will establish a framework to allow them to create their e-commerce portals. Small merchants will tell the RMA whatever commodities they want to offer in his portal, and the RMA will collect the data and maintain the framework so that each merchant's goods or services can be published on his e-commerce site. Merchants will have to worry about receiving orders and fulfilling them promptly. Furthermore, RMA could benefit small businesses by providing a delivery service to their customers.

Table 2 Some example studies for reviewing to develop the basis of the framework

Source studies	Contributions
Ingaldi and Ulewicz [16]	Understanding of basic e-business frameworks
Nguyen [17]	How various frameworks are being employed in various business model
Gregory et al. [15]	Example of marketing frameworks that can be developed to facilitate e-commerce
Wang and Han [18]	Overview understanding of how to implement e-commerce framework for small- and medium-sized enterprise
Yadav et al. [19]	How business website can be used to develop an e-commerce framework
Tolstoy et al. [20]	Understanding the development of international e-commerce in SME's
Yalan and Wei [21]	Evaluating e-commerce frameworks application

4.1 Framework Definition

To achieve the objectives above, we present a new e-commerce framework that allows small merchants to create their e-commerce platform with the help of the RMA. The RMA will handle all members' business. We have developed an e-commerce model geared toward merchants and backed by RMAs, in which merchants only require a cell phone and fax machine to take orders in their stores. Furthermore, the RMA would provide all of its members with the environment necessary to run a secure web server by sharing a single SSL certificate and a secure payment gateway, allowing all e-commerce portals to conduct all of their sales through the same secure payment gateway. As a result, all merchants will benefit from the RMA's partnerships with banks, while the Association's personnel will find it easier to administer the e-commerce infrastructure. For example, when a merchant has a ready order, he will send an SMS to the RMA's deliverer, instructing him to pick it up at his shop and transport it to the customer's location.

5 Discussion

Over the years, e-commerce adoption has widely grown in Saudi Arabia and beyond. E-commerce primarily encompasses the exchange of products and services electronically through the Internet. Primary e-commerce tools include social media, websites, electronic payment systems such as online bank transfers, credit cards, debit cards, and PayPal. Based on the numerous studies reviewed, e-commerce can be differentiated from traditional businesses through its distinct features, including ease of use, increased intractability between users and business, among others. These elements form the basis of the impacts of e-commerce technologies on business. Naturally, customer satisfaction is a vital aspect that influences the success or failure of a business. With an easy-to-use interface, customers can effectively communicate with a company and shop without any challenges. This is evident in websites that are optimized so that customers can use their mobile devices to shop. Notably, the ability of e-commerce technologies to positively impact businesses to this extent is attributed to the growth and adoption of the Internet in Saudi Arabia.

The Saudi environment has a defined set of laws and policies that govern the economic operations of entities, including e-commerce. The nation enforced the e-commerce law that compels entities to respect the privacy of the personal data of their consumers. Such legal structures enhance the efficiency of transactions between business entities.

Further studies might be designed to improve the use of multiple technologies for system design that meets dynamic demands of SMEs in this digital economy. For example, how the emerging technological functions such as the block chain (e.g., defined in [22]) can be used for SME's data security and transparency. Smart SME application development study can be conducted through adopting the design science research [23–25]. Example applications can be aligned to Big Data Analytics solution design for enhancing data-driven decision, e.g., other industries [26–29].

References

1. Hallikainen H, Laukkanen T (2018) National culture and consumer trust in e-commerce. Int J Inf Manage 38(1):97–106. https://doi.org/10.1016/j.ijinfomgt.2017.07.002
2. Statista (2021) E-commerce market in Saudi Arabia—Statistics and facts. Statista. https://www.statista.com/topics/7723/e-commerce-in-saudi-arabia/
3. Grbovic M, Radosavljevic V, Djuric N, Bhamidipati N, Savla J, Bhagwan V, Sharp D (2015) E-commerce in your inbox: product recommendations at scale. In: Proceedings of the 21th ACM SIGKDD international conference on knowledge discovery and data mining—KDD '15, pp 1809–1818
4. Alkhalil B, Siddiqui M (2018) Factors affecting Saudi consumer trust in e-Commerce: a quantitative analysis. Int J Comput Appl 182(25):41–45
5. Khan A (2016) Electronic commerce: a study on benefits and challenges in an emerging economy. Glob J Manage Bus Res 16(1)
6. Xuhua H, Elikem OC, Akaba S, Worwui-Brown D (2019) Effects of business-to-business e-commerce adoption on competitive advantage of small and medium-sized manufacturing enterprises. Econ Soc 12(1):80–366
7. Habboush TA, Alanazi BF (2020) The impact of electronic commerce on motivating the investment in the kingdom of Saudi Arabia. J Int Bus Res Market 5(5):13–27
8. Al Ghamdi R, Nguyen A, Jones V (2013) Wheel of B2C E-commerce development in Saudi Arabia. In: Robot intelligence technology and applications. Springer Berlin Heidelberg, pp 1047–1055
9. Purwati Y (2011) Standard features of e-commerce user interface for the web. Res World 2(3):77
10. Export.gov. (2020) Saudi Arabia—E-commerce. Retrieved from https://www.export.gov/apex/article2?id=Saudi-Arabia-ECommerce
11. Orloff S (2012) Saudi Arabia retail prospects and outlook for 2012. Retrieved from https://sachaorloff.files.wordpress.com/2012/01/saudi-arabian-retail-prospects-sacha-orloff-2012.pdf

12. Mazzarol T (2015) SMEs engagement with e-commerce, e-business, and e-marketing. Small Enterp Res 22(1):79–90
13. Helal M (2017) An investigation of the use of social media for e-commerce amongst small businesses in Saudi Arabia. Doctoral dissertation, University of Salford
14. Creswell JW (2005) Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Pearson Education Inc., Upper Saddle River, NJ
15. Gregory GD, Ngo LV, Karavdic M (2019) Developing e-commerce marketing capabilities and efficiencies for enhanced performance in business-to-business export ventures. Ind Mark Manage 78:146–157
16. Ingaldi M, Ulewicz R (2019) How to make e-commerce more successful by use of Kano's model to assess customer satisfaction in terms of sustainable development. Sustainability 11(18):4830
17. Nguyen TTN (2020) Developing and validating five-construct model of customer satisfaction in beauty and cosmetic E-commerce. Heliyon 6(9):e04887
18. Wang P, Han W (2021) Construction of a new financial E-commerce model for small and medium-sized enterprise financing based on multiple linear logistic regression. J Organ End User Comput (JOEUC) 33(6):1–18
19. Yadav N, Rajpoot DS, Dhakad SK (2019) Laravel: a PHP framework for e-commerce website. In: 2019 Fifth international conference on image information processing (ICIIP). IEEE, pp 503–508
20. Tolstoy D, Nordman ER, Hånell SM, Özbek N (2021) The development of international e-commerce in retail SMEs: an effectuation perspective. J World Bus 56(3):101165
21. Yalan Y, Wei T (2021) Deep logistic learning framework for E-commerce and supply chain management platform. Arab J Sci Eng 1–15
22. Prokofieva M, Miah SJ (2019) Blockchain in healthcare. Austr J Inf Syst 23:1–22
23. Genemo H, Miah SJ, McAndrew A (2015) A design science research methodology for developing a computer-aided assessment approach using method marking concept. Educ Inf Technol 22:1769–1784
24. Miah SJ, Gammack JG, McKay J (2019) A Metadesign theory for tailorable decision support. J Assoc Inf Syst 20(5):570–603
25. Miah SJ, McKay J (2016) A new conceptualization of design science research for DSS development. In: Proceedings of the 20th Pacific Asia conference on information systems (PACIS 2016), Taiwan. http://www.pacis2016.org/Abstract/ALL/758.pdf
26. Miah SJ, Vu HQ, Gammack J (2019) A Big-Data Analytics method for capturing visitor activities and flows: the case of an Island Country. Inf Technol Manage 20(4):203–221
27. Miah SJ, Vu HQ, Gammack J (2018) A location analytics method for the utilization of geotagged photos in travel marketing decision-making. J Inf Knowl Manag 18(1):1–13
28. Miah SJ, Hasan N, Gammack JG (2020) A Methodological requirement for designing healthcare analytics solution: a literature analysis. Health Informatics J 26(4):2300–2314
29. Miah SJ, Miah M, Shen J (2020) Learning management systems and big data technologies for higher education. Educ Info Technol 25:725–730

Cibercidadão: Evolution of Citizen Participation in Public Administration

Camila Z. Aguiar, Tasso M. Lugon, Delvani A. Mateus, Ádler O. S. Neves, and Uliane B. Bernadino

Abstract The Cibercidadão initiative began with the advent of digital transformation and the digital government law, which identified the need for efforts to improve digital public services. However, it was also observed that the improvement of digital public services would not be achieved individually with a view only from the public service, but together with the view of the citizen who uses this service. Thus, we identified that the citizen himself would be the most interesting part of this transformation process, as digital public services must be developed to meet the needs and expectations of citizens. In this scenario, we identified the existence of the Cibercidadão in society, that active and participative citizen of the public administration, which contributes to the improvement of public services. Thus, the Cibercidadão methodology places the citizen at the center of the digital transformation, sending ideas about technology and government, developing software solutions, testing and evaluating the solutions made available to society. Finally, the Cibercidadão is applied in a Government Program aimed at the development of innovative and citizen-centered software solutions, whose results are already promising.

Keywords Digital government · Public administration · Shared administration · Cybercitizen

1 Introduction

Digital transformation has been a key theme for the future of digital services provided by the government. Brazilian law 14.129/2021 establishes the "principles, norms and instruments to increase the efficiency of public administration, especially through

C. Z. Aguiar (✉) · T. M. Lugon · D. A. Mateus · Á. O. S. Neves · U. B. Bernadino
Innovation Laboratory-LINO, Institute of Information and Communication Technology of Espírito Santo, Vitória, Brazil
e-mail: camila.zacche.aguiar@gmail.com

T. M. Lugon
e-mail: tassolug@terra.com.br

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_41

reducing bureaucracy, innovation, digital transformation, and citizen participation" [1]. However, providing services to improve the lives of citizens is one of its main challenges and requires a better understanding of needs, capacities, limitations, and expectations of citizens. This law is an important milestone to follow in the footsteps of Estonia, which is a world reference in digital government and makes almost all public services available digitally to citizens, who do not need to go to government agencies, face queues, and bureaucracy [2].

In this scenario, Cibercidadão aims to bring government and citizens closer together based on the principles of shared management, inviting all citizens to be part of public administration with the application of information and communication technology (ICT). Given that digital transformation is an arduous and time-consuming process that does not always meet the expectations of the citizen, Cibercidadão supports in the development of innovative and citizen-centric software solutions to provide qualified and inclusive digital public services. For this, citizens are invited to submit ideas related to ICT and government, which will be analyzed and implemented as technological solutions with citizen participation. Then, the citizen takes part in the test of the solution in order to verify that the expectations were met in terms of need, usability and accessibility. Finally, with the use of the service made available to the citizen, it is expected the citizen's participation in evaluations and feedbacks for the continuous improvement of the services.

This article presents the fundamentals of the Cibercidadão methodology, as well as its application in a government program aimed at the development of innovative and citizen-centered software solutions. Since the program is aimed at all citizens, including those with disabilities, it considers the participation of different citizen profiles (students, elderly, disabled, and others) and implements technological accessibility resources (screen reader, signal assistant, audio assistant, and assistant virtual). The rest of this article is organized as follows. Section 2 presents the citizen participation. Section 3 discusses the related work. Section 4 presents the methodology to be used in designing new citizen-centric products. Section 5 presents the results case study of the application of the Cibercidadão. Section 6 presents the results and discussions about the Cibercidadão Program. Finally, Sect. 7 presents conclusions and future work.

2 Citizen Participation

Citizen participation in public administration originated in the late 1980s by the Organization for Economic or Economic Cooperation and Development (OECD) and was called customer-focused administration. In the early 1990s, Brazil began to use this concept comprehensively in public administration, being called citizen-focused administration. The objective is to offer efficient and quality public services that meet the needs of citizens. With this new administration, the services provided try to be clear and precise, including resources from the public sector to the demands of the citizen [3].

The relationship between communication and politics presents concepts related to public communication [4]. On the one hand, the Habermasian concept of public communication takes place in the public sphere, based on the idea of social mobilization [5]. On the other hand, public communication is defined in five dimensions [4, 5]: **Politics**: is related to the "government" legislative and the construction of public goods; **Media**: takes place in the panoramas of the media, oriented toward information management and public agenda, as well as cultural processes; **State**: is related to communicative interactions between government and society; **Organizational**: organizations being public or private, the interests of these groups seek to predominate and impose their meanings. It has a corporate character, instances, and benefits of collective interest; **Social life**: are the spontaneous or non-spontaneous correlations of associations and social movements, which have collective or group mutuality, launching proposals of collective and public interest.

3 Related Work

Study Alves' verified the process of creating government portals in governmental IT companies in the 25 states of Brazil and found that the managers' concern is in relation to the qualification of the developers, in relation to the designs there was no such concern, one of the questions to managers was the following: "*Is there a professional who takes care of the design of the screens and who does some research with the users?*" there were no positive responses. The products are developed without using the user-centered design methodology, all the portals presented accessibility and usability issues [6].

What corroborates Harrison et al. [7] user-centric designs include rapid ethnography, focus group, interview, drawing technique, paper prototyping, and high-fidelity prototyping. This type of analysis complements formal user ratings. This approach enriches user-centric design, which typically focuses on understanding in context and producing sketch designs.

For Cunha [8], information and communication technology (ICT) in the public sector in the area of digital, must be accompanied by technological innovation to propose improvements in public service (e-services). All citizens must not be assisted in the same way, with no privilege or compensation for social status, promoting citizenship.

For Cristóvam [9], ICTs have the potential to assist innovation and encourage the provision of consistent and update public services that society is about to use. Digital government must comply with the principles of (i) efficiency, aiming for maximum satisfaction of the citizen user; (ii) universality, maximizing the scope of availability of such services; and (iii) timeliness, ensuring that technological advances. ICTs should bring about the digital inclusion of socially vulnerable, handicapped, and low-income classes.

4 Methodology

The Cibercidadão places the citizen at the center of the digital transformation and, therefore, define the methodology comprising the following phases in Fig. 1: collection, development, testing, and evaluation, which, based on their integrations, are capable of generating new services and improvements in services and processes.

In the first phase, the **Collection Phase**, the citizen witnesses the public service and sends ideas involving technology and government. Ideas are analyzed by experts and stored in the ideas base, categorizing them according to the subject and their feasibility.

In the second phase, the **Development Phase**, viable ideas are deepened and directed toward development, which can take place through hackathons, research, or institutional partnerships. For the hackathon, citizen ICT students from different know-how participate in a programming marathon to develop technological solutions from ideas submitted by citizens in a short period of time. From the winning solutions, a final product is designed to serve the entire society, materializing the idea sent by the citizen. In this case, students participate in the construction of the technological solution so that academia gets closer to real problems. For the research, citizen researchers work in the study and discovery of technological solutions based on ideas submitted by citizens. In this case, the government has the opportunity to apply science to the solution of ideas sent by the citizen, as well as the academy has the opportunity to leave the theoretical level and apply its findings in practice. For the partnerships, academic, public, and private institutions join efforts to develop solutions in order to meet the citizens' ideas.

In the third phase, **Testing Phase**, citizens are invited to be beta testers of the solutions developed, acting as end-users of the service offered before it is launched. The tests are carried out with citizens of different profiles, including those with disabilities, prioritizing usability and accessibility. The results of the evaluations are stored in the test base and used for adjustments and improvements to the solution under development.

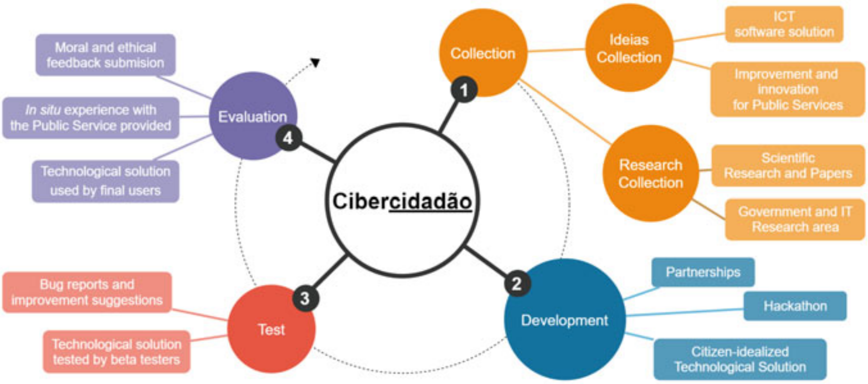

Cibercidadão
Collection
1
Ideias Collection
ICT software solution
Improvement and innovation for Public Services
Research Collection
Scientific Research and Papers
Government and IT Research area
Development
2
Partnerships
Hackathon
Citizen-idealized Technological Solution
Test
3
Bug reports and improvement suggestions
Technological solution tested by beta testers
Evaluation
4
Moral and ethical feedback submision
In situ experience with the Public Service provided
Technological solution used by final users

Fig. 1 Cibercidadão methodology

In the fourth phase, the **Evaluation Phase**, the solution developed and tested in the previous phases is made available to society. As citizens use the solution and take advantage of the public service offered, they send feedback and evaluation about the solution and contribute to the continuous improvement of the solution and the delivery of public services.

5 Case Study of the Application of the Cibercidadão

Cibercidadão was applied as a government program in the state of Esprito Santo, in Brazil, which has about 4 million people and approximately 1 million people with disabilities. In honor of the methodology, the program was called Cibercidadao Espírito Santo and has a Web portal to communicate with citizens and monitor the phases.

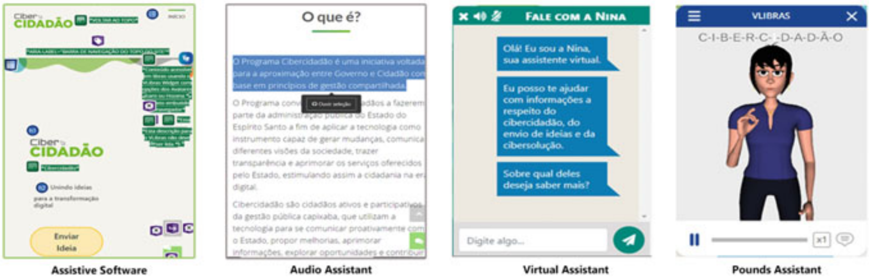
5.1 Web Portal Cibercidadão

Since Web portal intends to involve all citizens, including those with disabilities, they has technological resources for accessibility and usability (Fig. 2). Accessibility features were implemented following the national e-MAG (Brazilian Government Accessibility Model) [10] and international Web Content Accessibility Guidelines (WCAG) [11] guidelines, which allow keyboard navigation and navigation using screen readers, enabling user interactions.

One such feature is the **Pounds Assistant** which translates text into sign language. To use it, just click on the blue icon in the right corner of the page. Then, select the text and wait for the content to translate into Libra signs. Another feature is the **Audio Assistant**, responsible for converting text to sound as well as sound to text. To use it, you must first select the content, click on "Listen to Selection" and wait for the assistant to read it. An **Virtual Assistant** is also part of the resources available on the portal to serve the citizen, clarifying doubts and directing to the program phases. In addition to these features, the portal is also configured for the use of **Assistive Software** that identifies website elements and reads the content for people with disabilities, who have difficulty consuming written information.

To ensure that the resources made available on the portal serve the citizen, the resources were evaluated in an automated way through tools and manual through experts, including with the participation of the citizen (people members of the project).

The technological architecture used to implement the Web portal is a client-server, with C# programming language. Natural language processing heuristics are applied from a definition of writing in a domain-specific language. Furthermore, features are implemented and integrated with libraries related to the translation of texts, pounds, and audio.



O Programa Cibercidadão é uma iniciativa voltada para a aproximação entre Governo e Cidadão com base em princípios de gestão compartilhada.

O Programa conv dãos a fazerem parte da administração pública do Estado do Espírito Santo a fim de aplicar a tecnologia como instrumento capaz de gerar mudanças, comunica diferentes visões da sociedade, trazer transparência e aprimorar os serviços oferecidos pelo Estado, estimulando assim a cidadania na era digital.

Cibercidadão são cidadãos ativos e participativos da gestão pública capixaba, que utilizam a tecnologia para se comunicar proativamente com o Estado, propor melhorias, aprimorar informações, explorar oportunidades e contribuir

Olá! Eu sou a Nina, sua assistente virtual.

Eu posso te ajudar com informações a respeito do cibercidadão, do envio de ideias e da cibersolução.

Sobre qual deles deseja saber mais?

Fig. 2 Technological resources of the Cibercidadão portal

5.2 *Application*

The Web portal was launched to receive the ideas submitted by the citizen, that is, collection phase. This phase lasted three months and adopted the following strategy: filter, classification, and analysis of ideas. All ideas received are initially filtered by a support technician according to the content, namely random content, incomplete content, or content involves technology.

After filtering, in the classification, IT analysts check whether the idea that involves content technology corresponds to an existing solution improvement, process improvement, or innovative idea. After classification, the idea is analyzed according to the criteria of creativity, technical analysis, ease of implementation, potential for implantation, and impact on the citizen, being developed through hackathons, educational institutions, public bodies, and by the institution itself. Each idea is scored from 0 (weak) to 5 (strong) for each criterion.

In the development phase, the program executed hackathons with graduate students, who produced a software solution for one of the ideas submitted by the citizen. For the testing phase, citizens sign up to test the software, and the evaluation phase takes place through citizen feedback sent by the solutions made available to society.

6 Results and Discussions

The Cibercidadão program presented in Sect. 5, which applies the Cibercidadão methodology and offers a Web portal for communication, is online for just four months and is already showing promising results.

In the collection phase, the program received around 147 ideas submitted by the citizen, [Table 1, Quantity (Qt)], of which 33% have random content and 67% are related to the Program's objective. Of these related ideas, 40 with existing solutions, 10 with solution improvement, and 18 with innovation ideas. The Innovation Ideas related to new services presents ideas for usability problems and lack of functionality in the websites of the State of Espírito Santo, such as health, education, traffic, and

Table 1 Category of ideas received by the program

Category	Description	Qt
Random content	No information—text without information, repeated letters	4
	Random subject—subject out of context	20
	Inappropriate—spam and insults	25
Incomplete content	Has no description needed to deduce a solution	3
Technology content	Creation of new services	18
	Ideas about process optimizations	40
	Availability of Wi-Fi in schools and neighborhoods	27
	Solution improvement	10

controllership. For example, one of the ideas is the creation of an application that informs the amount of blood in the banks and invites the donor to carry out the donation procedure whenever the gap time is over.

In the development Phase, the program carried out a hackathon with computer students who produced a software solution for one of the ideas submitted by the citizen, namely *Integrated FAQ that allows you to search and access information related to government services*. The solution produced by the students at the hackathon is being transformed into a software product to be offered to society, being tested and subsequently evaluated.

7 Conclusion and Future Work

The Cibercidadão methodology made it possible for the Cibercidadão program to be a pioneer in Brazil in adopting a methodology for capturing ideas perceived by citizens and applying them to society, promoting shared management, research conducted in other 25 States did not find a program similar to this one. In addition, an analysis carried out on all institutional websites in the state found that there are no accessibility and usability features implemented on the websites (report available on the project website[1]). The program is a pioneer in the State of Espírito Santo in providing a fully accessible Web portal for people with disabilities, including providing a virtual assistant, audio, and pounds. These resources are capable of providing citizen engagement to the program. Citizen engagement is the crucial point for the success of initiatives promoted by the government [12].

[1] https://lino.prodest.es.gov.br/esgovacessivel.

The ideas submitted by citizens are simple, but they can bring added value and satisfaction to society [13]. The program, despite still being in the initial stage, is promoting the opportunity for society to express the problems day to day in the use of digital public services by taking positive feedback from a range of citizens, even though some citizens feel excluded due to a lack of access to computers, smartphones, and others.

The next phases of the program that are being implemented are the test phases, which will be responsible for testing the developed solution, and the evaluation phase, which will be responsible for citizen feedback on the digital public service offered. As future work, the solutions developed will be analyzed quantitatively and qualitatively based on feedback from citizens.

References

1. Governo Brasileiro (2021) Governo digital e para o aumento da eficiência pública. https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132
2. Anthes G (2015) Estonia: a model for e-government. Commun ACM 58(6):18–20
3. Coutinho MJV (2014) Administração pública voltada para o cidadão: quadro teórico-conceitual. Rev do Serviço Público 51(3):40–73. https://doi.org/10.21874/rsp.v51i3.331, https://revista.enap.gov.br/index.php/RSP/article/view/331
4. Jaramillo López J (2004) Modelo de comunicación pública organizacional e informativa para entidades del estado. USAID/Casals & Associates Inc., MCPOI Bogotá
5. Koçouski M (2012) Comunicação pública: construindo um conceito. Comunicação pública: interlocuções, interlocutores e perspectivas São Paulo: ECA/USP, pp 71–96
6. Vasconcelos Alves A (2014) Design centrado no cidadão: um modelo para a gestão de design em governo eletrônico. En: Interaction South America (ISA 14) : 6ta Conferencia Lationamericana de Diseño de Interaccion
7. Harrison MD, Masci P, Campos JC (2021) Balancing the formal and the informal in user-centred design. Interacting Comput 33(1):55–72. https://doi.org/10.1093/iwcomp/iwab012, https://doi.org/10.1093/iwcomp/iwab012, https://academic.oup.com/iwc/article-pdf/33/1/55/38495883/iwab012.pdf
8. Cortez da Cunha MAV, Miranda PRdM (2013) The use of ICT by governments: a proposed research agenda based on the academic production an don national practice. Organizações & Sociedade 20(66). https://periodicos.ufba.br/index.php/revistaoes/article/view/8843
9. da Silva Cristóvam JS, Saikali LB, de Sousa TP (2020) Governo digital na implementacao de servicos publicos para a concretizacao de direitos sociais no brasil/digital government in the implementation of public services for the realization of social rights in brazil. Sequencia: estudios juridicos e politicos, pp 209–243
10. Governo Brasileiro (2014) emag - modelo de acessibilidade em governo eletroico. Retrieved 16 Feb 2021 from http://emag.governoeletronico.gov.br/
11. World Wide Web Consortium WAI (2018) W3c. web content accessibility guidelines (wcag) 2.1. Retrieved 20 Feb 2021 from https://www.w3.org/TR/WCAG21/
12. Oliveira C (2020) Proposed solutions to citizen engagement in virtual environments of social participation: a systematic review. Int J Electron Governance 12(1):76–91. https://doi.org/10.1504/IJEG.2020.106994, https://www.inderscienceonline.com/doi/abs/10.1504/IJEG.2020.106994, https://www.inderscienceonline.com/doi/pdf/10.1504/IJEG.2020.106994
13. Pagnan AS, Simplício GC, Santos VC (2019) Design centrado no usuário e seus princípios éticos norteadores no ensino do design. Estudos em Design 27(1)

A Low-Cost and Energy Autonomous IoT Framework for Environmental Monitoring

Vasileios Galafagas, Fotios Gioulekas, Panagiotis Maroulidis, Nikolaos Petrellis, and Panagiotis Katsaros

Abstract The emergence of IoT devices that support sensor technology has gain much attention for their integration into smart city applications to improve citizens' quality of life. In industrial territories, people that suffer from chronic respiratory diseases, e.g., chronic obstructive pulmonary disease, asthma, occupational lung diseases and pulmonary hypertension require special care, targeted information and efficient treatment, when the environment deteriorates their condition. This article presents the design of an IoT framework that wirelessly connects devices of low-cost, low-power consumption and integrates multi-sensor measurement capabilities (CO_2 concentration, humidity, temperature, particulate matters concentrations) with an open-source IoT platform aiming to alert the aforementioned population, when the combination of aerial pollution and weather conditions severe impact their daily activities. The energy autonomy of the IoT devices that are connected via wireless sensor network is explored and utilized. Finally, we evaluate the functionality and the accuracy of the low-cost sensors and demonstrate how proper filtering can improve their performance and mitigate problems stemming from outage times. For the latter, we have evaluate the effectiveness of forecasting algorithms like ARIMAX, LSTM and PROPHET on the measurement data.

V. Galafagas (✉)
General Evening High School of Volos, 38222 Volos, Greece
e-mail: mail@lyk-esp-volou.mag.sch.gr

F. Gioulekas
Directorate of Informatics, 5th Regional Health Authority, 41110 Larissa, Greece
e-mail: fogi@dypethessaly.gr

P. Maroulidis · P. Katsaros
Department of Informatics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece
e-mail: maroulidi@csd.auth.gr

P. Katsaros
e-mail: katsaros@csd.auth.gr

N. Petrellis
Department of Electrical and Computer Engineering, University of Peloponnese, 26334 Patras, Greece
e-mail: npetrellis@uop.gr

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_42

Keywords Low-cost multi-sensor node · Environmental monitoring · IoT gateway · Time-series data · IoT platform

1 Introduction

Changes in air quality, and especially in areas of high humidity and/or moderate to high level of temperature, affect severely the quality of life of people that suffer from chronic obstructive pulmonary disease, asthma, occupational lung diseases, pulmonary hypertension and similar chronic diseases. A representative example of such a territory is the Greek coastal city of Volos, where past scientific analyses of the air consistency revealed that suspended particulate matter (PM) with aerodynamic diameter equal to 10 μm (PM_{10}) and 2.5 μm ($PM_{2.5}$) along with the CO_2 emissions indicated pollutants that cause health disorders in heart and respiratory system [1]. A similar assessment on long-term air quality data revealed that suspended particulate matter (PM_{10}) is a pollutant that may cause health disorders [2].

The aforementioned analyses require an underlying architecture, within a smart city framework, to collect data in real-time from environmental sensors, located at various city districts, and deliver alerts thus, assisting regional health authorities and physicians to guide the vulnerable citizens' group. To this end, wireless sensor network solutions along with forecasting algorithms for monitoring pollution level in agglomerated areas, while targeting a low-energy consumption, have been applied [3–6]. The advantage of small, low-cost, wireless and energy autonomous sensor nodes is their portability compared to modular and expensive systems [7]. However, the reliability and accuracy of low-cost sensors requires evaluation and constant monitoring. In addition, several research efforts have combined low-cost sensors with IoT platforms for air quality evaluation in smart city applications [8–12].

This work presents the development and implementation of low-cost multi-sensor nodes with energy autonomy and low-power consumption to monitor environmental conditions. Our target is to decrease energy consumption and increase battery lifetime to ensure portability. We focus on the architectural design of an efficient, secure and scalable wireless network topology to connect the nodes and transmit the sensor data over the Internet to an IoT platform using publish-subscribe protocols [13]. The IoT platform [14, 15] is based on open-source solutions and stores the received time-series data while providing real-time dashboards to the users. We evaluate the performance of the sensors by comparing them against reference data and explore filtering methods to improve quality and accuracy in comparison with the aforementioned prior works. Furthermore, issues concerning periods without data reception, e.g., in case of sensor node outage, are addressed while various prognostic algorithms are evaluated for forecasting purposes [16–18].

2 Design of Multi-sensor Node for Low-Energy Consumption

The architecture of the proposed multi-sensor node, which is built using off-the-shelf components, is shown in Fig. 1. A 3.3 V ARDUINO unit is interfaced with four sensors, namely CO_2 [19], temperature & humidity [20], $PM_{2.5}$ & PM_{10} [21] and light-dependent resistor sensors [22], and processes six data values for CO_2 concentration, humidity, temperature, particulate matters concentrations ($PM_{2.5}$ & PM_{10}) and light intension, respectively. A low-power Xbee module [23], connected via the UART port to the ARDUINO unit (Fig. 1), was configured as a unicast device and is used to transmit the acquired data to an Xbee destination device, thus forming a wireless sensor network based on the Zigbee communication protocol [23]. The destination device eventually sends the aggregated data over the Internet to an IoT platform. A power supply circuit (see Fig. 1) has been developed and integrated, in order to maintain energy autonomy of the wireless multi-sensor node. It features a nominal 6 V (7 V max measured value) solar cell that can generate a maximum power of 3.15 W (7 V * 450 mA), a battery charger, a rechargeable Li-Ion battery (with a capacity of 5000 mAh), a Power Timer circuit and a voltage booster. The battery charger [24] acts as a constant-current/constant-voltage linear charger and is used to charge the Li-Ion battery. The TPL5110 Nano Power Timer IC [25] is used for power gating and thus, to enable the power supply line, in order to drastically reduce the overall system standby current during the sleep time. It provides selectable timing intervals from 100 ms to 7200 s, and it is designed for power gating applications.

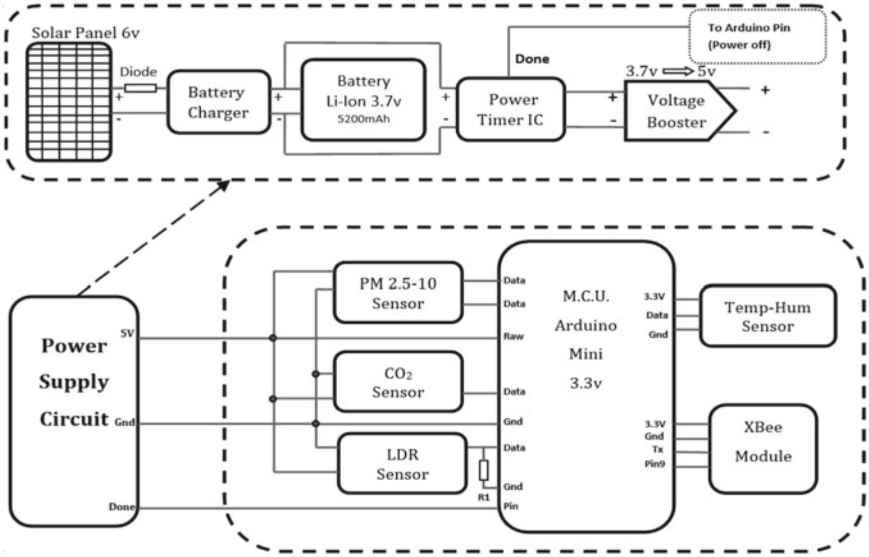


Fig. 1 Architecture of the multi-sensor node with energy autonomy

Due to 4.3 V output voltage of the Li-On battery, a 0.9–5 V voltage booster (DC-DC converter) was used to power both the ARDUINO Pro Mini microcontroller (MCU) and the CO_2 sensor [26], which require 3.3 V and 5 V power supply, respectively.

Our focus is to achieve both a constant rate of data acquisition from the sensors and a low-power consumption, in order to increase the energy autonomy of the multi-sensor node. Alternatively, usage of batteries without a solar cell to charge them, was prohibitive, as the total current exceeded 135 mAh (fully active sensor node). Even with a battery of 5000 mAh, the sensor node could remain active almost for only 2 days before it runs out of charge. The ARDUINO Pro Mini (3.3 V, 8 MHz) consumes 5.1 mA, when it is powered on and 1.3 mA while in sleep mode [23]. The subsystems, microcontroller, CO_2 sensor, particulate matter sensor and LDR sensor, are powered directly by the proposed power supply circuit that produces a steady output of 5 V. The CO_2 sensor requires a preheating time greater than 1 min, before the microcontroller gets its first value. This type of sensor is based on infrared technology, and after a working period of 20 s it needs a preheating time of 55 s. During this preheating period, a spike current of 95 mA every 5 s increases dramatically the power consumption. To further reduce power consumption, a software algorithm was applied to periodically force the Xbee module, the sensor units and the ARDUINO MCU to enter the sleep mode. Since the Xbee device requires 40 mA to operate [23], the ARDUINO was programmed to activate the Xbee hibernation mode. When the device is in hibernation mode, the Xbee device operating current is less than 1 mA [23]. Furthermore, we also used the Lightweight Low-Power ARDUINO Library [27] to drastically reduce power consumption of the MCU, since it allows to disable many subsystems, among others the Analog/Digital Converter and BOD (Brown Out Detection) circuits, by using the "*Low-Power. Power Down (SLEEP_8 S, ADC_ OFF, BOD_ OFF)*" instructions. Since our sensor node transmits data every 262 s, the power down time was adjusted to the maximum time that would be beneficial for power reduction that can be achieved in each duty cycle (1 min).

Figure 2 depicts the operational stages of the designed multi-sensor node. The ARDUINO MCU loops to sustain the power down mode. When entering the wake up mode, it collects all sensor data and transmits them over the Xbee module (using the UART port) to the corresponding destination (Router). Specifically, the timer circuit powers on the sensor node, then the particulate matters (PM) sensor and the Xbee device enters the sleep mode, and afterward the MCU goes to power down state, while the CO_2 sensor remains active for preheating. After a certain period of time, the MCU, the PM sensor and the Xbee device wake up and the MCU gets the data values from the sensors and forms a fixed length data packet. Then, the PM sensor enters the sleep mode and the Xbee device transmits data packet to the Router module that is described in next sections. Finally, the MCU triggers the timer circuit, which in turn switches off the multi-sensor node.

For the outlined node design, we measured the current consumption using a multimeter and an oscilloscope. As shown in Table 1, the measurements revealed that each duty cycle lasts 262 s. The duty cycle includes three operation states plus the fourth state in which the node is switched-off. A new duty cycle starts, when the power-time circuit powers on the node again. The captured current consumption

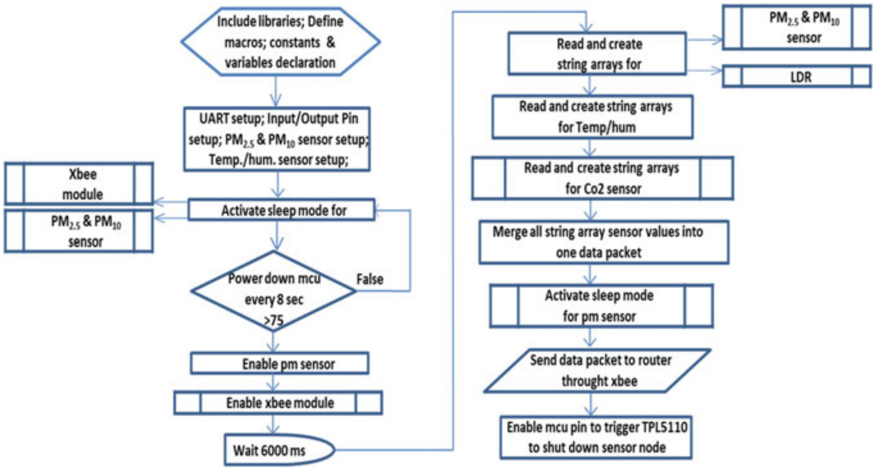

Include libraries; Define macros; constants & variables declaration
UART setup; Input/Output Pin setup; PM$_{2.5}$ & PM$_{10}$ sensor setup; Temp./hum. sensor setup;
Xbee module
PM$_{2.5}$ & PM$_{10}$ sensor
Activate sleep mode for
Power down mcu every 8 sec >75
False
Enable pm sensor
Enable xbee module
Wait 6000 ms
Read and create string arrays for
PM$_{2.5}$ & PM$_{10}$ sensor
LDR
Read and create string arrays for Temp/hum
Read and create string arrays for Co2 sensor
Merge all string array sensor values into one data packet
Activate sleep mode for pm sensor
Send data packet to router throught xbee
Enable mcu pin to trigger TPL5110 to shut down sensor node

Fig. 2 Multi-sensor node task graph

Table 1 Operation states of the multi-sensor node

Operation states	Multi-sensor node's subsystems states	Current (mA)	Duration (s)
1	PM sensor and Xbee unit are in sleep mode MCU is powered down CO_2 sensor is initialized	12	20
2	PM sensor and Xbee unit are in sleep mode MCU is powered down CO_2 sensor is in preheating mode	115	55
3	MCU is ON The sensors and the Xbee unit are ON Node reads data and transmits data	135	7
4	The whole Node is powered off	0	180

analysis within a duty cycle vs. time is shown in Fig. 3. The calculated average power consumption over time is $I_{\text{avg}} = [(I_{1\text{-ON}} * t_{1\text{-ON}}) + (I_{2\text{-ON}} * t_{2\text{-ON}}) + (I_{3\text{-ON}} * t_{3\text{-ON}}) + (I_{4\text{-ON}} * t_{4\text{-ON}})]/(t_1 + t_2 + t_3 + t_4) = 10.9$ mA, which is considerably lower than the 135 mA required for the designed node to operate without applying the energy reduction algorithm described above. Therefore, the energy autonomy of the node is significantly increased to 16 days (without the support of the solar panel).

3 IoT Platform Architecture and Network Topology

The overall architecture of the proposed IoT framework is shown in Fig. 4. It comprises: (i) the topology of the wireless sensor network (WSN) with their

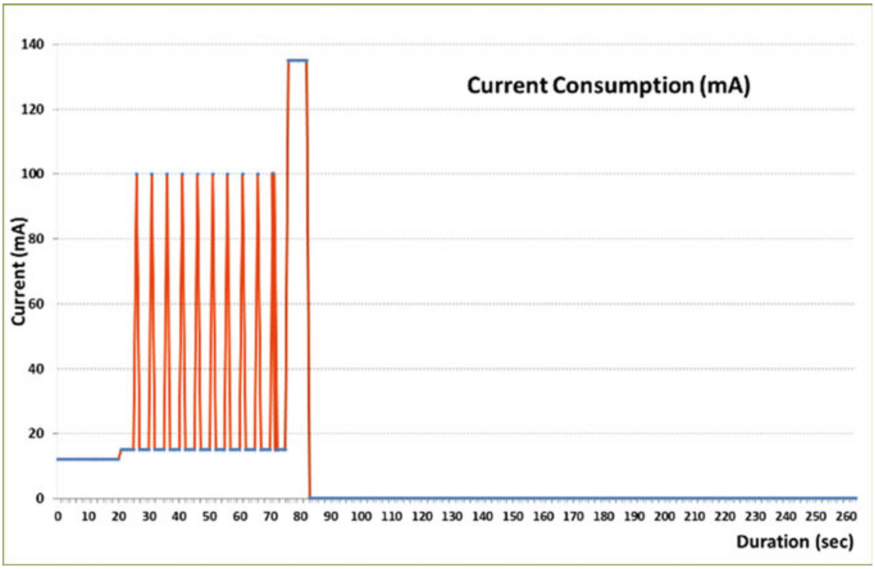


Fig. 3 Multi-sensor node current consumption per duty cycle

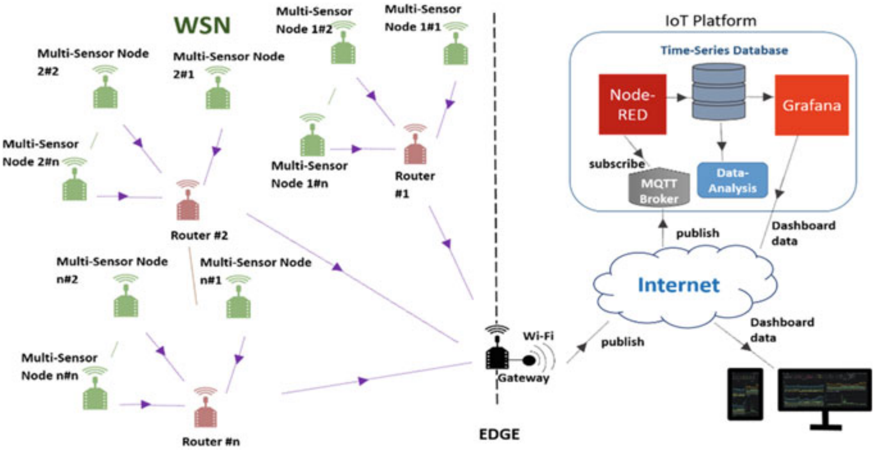


Fig. 4 Overall architecture of the implemented IoT framework

constituent multi-sensor nodes placed, according to the urban planning, in districts that sunlight is present to ensure the energy autonomy, (ii) the Edge communication through an IoT gateway, and (iii) the IoT platform, which eventually processes

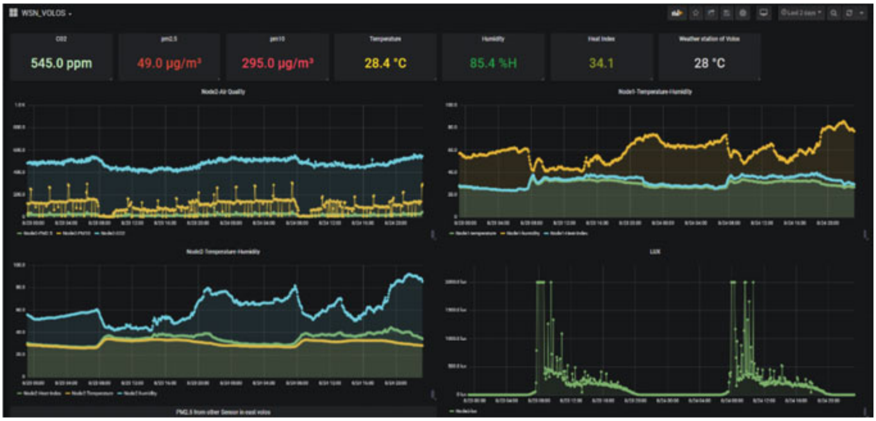


Fig. 5 Dashboard that shows latest measurements on top and plots with time-series values for two consecutive days

and analyzes the measurements to visualize them in the users' devices (i.e., smartphones and personal computers). We note that the reliability of environmental pollutant measurements depends on the sensor node placement, as well as on the sensor quality and accuracy (Fig. 4).

The WSN topology incorporates the role of the router, which directly collects the data from the sensor nodes, and then sends it to the gateway device (thus covering more distance), instead of having the sensor nodes transmitting their data directly to the gateway device. The network architecture is of a clustered tree structure. Each multi-sensor node sends a data frame consisting of a concatenated string of the measurements and the predefined node_id to a specific router using the destination MAC address. The routers and the gateway are configured to keep alive their child MAC address table for faster join network eliminating the possibility of losing data packets. This scalable mechanism is adopted to achieve better geographic dispersion and in order to capture various microclimatic conditions. The router and gateway devices are based on the multi-sensor node architecture of Fig. 1, after removing the sensors, while for the gateway device adding a Wi-Fi shield. For security purposes, we enabled AES encryption and device authentication in the WSN network [23]. Thus, the gateway transforms the received Xbee data packet to an MQTT frame comprising a topic and data and send via an SSL/TLS connection to the MQTT broker based on the public-subscribe protocol [13]. The proposed IoT platform is based on a time-series database that stores the received data, as well as on the Node-RED [14] and the Grafana [15], open-source solutions for data processing and visualization to efficiently provide alerts and a private dashboard to end-users (physicians, health authorities) and to citizens via the public interface https://iot-city.weebly.com/. Figure 5 illustrates the dashboard of the IoT platform where the end-users are signed in with secure accounts.

4 Evaluation of the Performance of Sensors and Forecasting

Two multi-sensor nodes were deployed at specific locations in the city of Volos, which allowed us to evaluate the performance of our IoT framework. Specifically, we analyzed the sensor data that have been collected from September 2019 until December 2020. Within the scope of the performance and accuracy evaluation of the sensor data, we used as reference the data obtained from the meteorological station of Volos (http://penteli.meteo.gr/stations/volos/). Our analysis was supported by the Node-RED configurations and was focused specifically on the temperature data. We noticed that due to sensor nodes outage periods (e.g., sensor's overheating or malfunctions) at specific times during the study period, there were missing measurements or outliers. Additionally, for some days we observed a high number of measurements for a relatively small timeframe, while for other days we only had a single measurement. To address these problems, we performed data imputation by calculating the mean value per day and per node and through merging the two time-series data from node-1 and node-2. However, there were still some days without any value, which directed us to perform linear interpolation to fit the curve of the merged mean temperature values (hereafter merged data). On the other hand, we also calculated the mean value per day for the reference temperature. Figure 6 shows the daily mean values for the reference sensor, for each one of the two nodes and for the merged data.

As evaluation criteria, we used the Pearson squared correlation coefficient (R^2) and the mean absolute error (MAE), in order to compare merged data from the sensor against the reference data (we target to high R^2 and low MAE values). Additionally, we also computed the 3-day moving average, the weekly moving average and the monthly moving average, and our findings are shown in Table 2. In overall, it seems

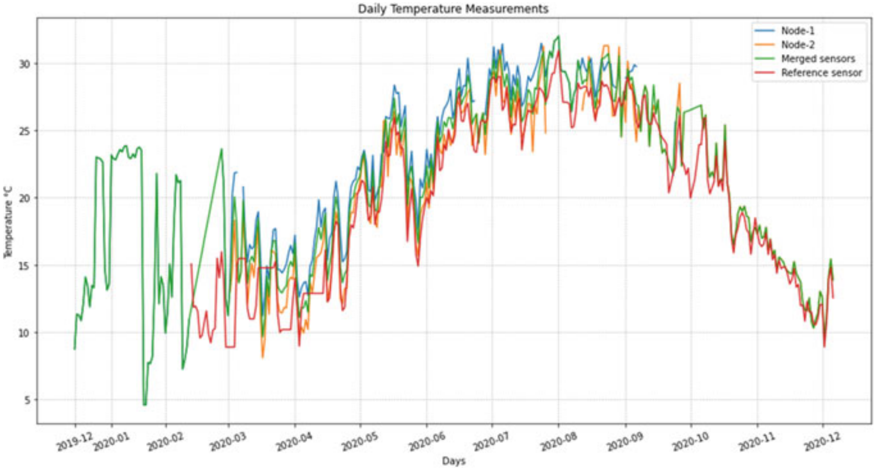


Fig. 6 Daily mean values for temperature data (node-1, node-2, merged data, reference sensor)

Table 2 Comparison of the merged data against reference temperature data

Criteria	Daily mean	3-days moving average	Weekly moving average	Monthly moving average
R^2	0.818	0.839	0.846	0.751
MAE	1.891	1.777	1.773	2.287

Table 3 Comparison of the forecasting algorithms on the temperature data

Criteria	LSTM	PROPHET	ARIMAX
R^2	−0.817	−0.104	−0.558
MAE	1.553	0.96	1.535

that the 3-days and weekly moving average filtering perform slightly better and allows us to conclude that the data generated from the low-cost sensors is almost identical to the reference data, and effectively capture the same temperature observations. This implies that our implemented multi-sensor nodes can be efficiently used for environmental monitoring. Furthermore, we have used daily moving mean values as input to the forecasting algorithms (LSTM [16], PROPHET [17], ARIMAX [18]). The LSTM algorithm was executed by removing the trend and keeping the seasonality. We used 30 lags (30 previous days, 1 month) to predict the next and ran 10 separately LSTM models. The PROPHET algorithm was executed by setting the parameters daily seasonality to true, seasonality mode to multiplicative, monthly seasonality to true, changepoint_prior_scale to 0.9, and seasonality_prior_scale to 50 (Table 3).

Table 3 depicts the calculated R^2 and MAE values between the predictions produced from the aforementioned algorithms and the reference sensor data. The negative R^2 means that the correlation between the predictions and the data from the reference sensor is really low and the three prediction models require more data. The results that the three forecasting models also depend on the data imputation. Therefore, it is deduced that it is very important to sustain the adequate performance in IoT framework like ours, so that sensor nodes produce data efficiently without any gaps due to sensors' outages.

5 Conclusion

Current work presents an efficient way to measure air pollutants in a smart city environment and capture the microclimatic variations using low-cost sensors and devices as well as open-source IoT platform solutions. The utilized low-power techniques and energy autonomous mechanisms are described in detail along with the overall low-cost IoT framework. Furthermore, we demonstrate how low-cost sensors can improve their performance and accuracy by employing filtering algorithms. Moreover, forecasting algorithms like LSTM and Prophet are evaluated for the prognostic efficiency on the measurement sensor, and we show how multi-sensor nodes outages can be mitigated with proper data imputation from neighbor nodes. Future work includes the support of mesh topologies and LoRa wide-area network modulation techniques to extend further the coverage area in a fault-tolerant mode while collecting data for more than a year. Additional updates will support the filtering mechanisms in the multi-sensor nodes rather than the IoT platform itself while the application of machine-learning techniques on the edge will be also evaluated.

Acknowledgements This research has been co-funded by the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH-CREATE-INNOVATE II (project code:T2EDK-02617).

References

1. Moustris K, Proias G, Larissi I, Nastos P, Koukouletsos K, Paliatsos A (2016) Health impacts due to particulate air pollution in Volos City, Greece. J Environ Sci Health, Part A 51(1):15–20
2. Moustris K, Proias G, Larissi I, Nastos P, Koukouletsos K, Paliatsos A (2014) Air quality prognosis using artificial neural networks modeling in the urban environment of Volos, Central Greece. Fresenius Environmental Bulletin (23), 2967–2975
3. Malche T, Maheshwary P, Kumar R (2019) Environmental monitoring system for smart city based on Secure Internet of Things (IoT) architecture. Wirel Pers Commun 107:2143–2172
4. Cao Pham T, Bich Vo H, Quang Tran N (2021) A design of greenhouse monitoring system based on low-cost mesh Wi-Fi wireless sensor network. In: 2021 IEEE international IOT, electronics and mechatronics conference (IEMTRONICS), Toronto, Ontario, Canada, pp 1–6
5. Buelvas JHP, Avila FEB, Gaviria NG, Munera DAR (2021) Data quality estimation in a smart city's air quality monitoring IoT application. In: 2021 2nd sustainable cities Latin America conference (SCLA), Medellín, Colombia, pp 1–6
6. Putra PRP, Wibisono G (2021) Intelligent street light pole planning based on LoRa Technology in Depok City. In: 2021 International conference on green energy, computing and sustainable technology (GECOST), Miri, Malaysia, pp 1–5
7. Laboratory Evaluation of Low-Cost Air Quality Sensors. http://www.aqmd.gov/docs/default-source/aq-spec/protocols/sensors-lab-testing-protocol6087afefc2b66f27bf6fff00004a91a9.pdf, last accessed 2021/09/27
8. Castell N, Dauge FR, Schneider P, Vogt M, Lerner U, Fishbain B, Broday D, Bartonova A (2017) Can commercial low-cost sensor platforms contribute to air quality monitoring and exposure estimates? Environ Int 99:293–302
9. Array of Things Project. https://arrayofthings.github.io/, last accessed 2021/09/27
10. Opensense Project. https://gitlab.ethz.ch/tec/public/opensense, last accessed 2021/09/27
11. EveryAware Project. http://www.everyaware.eu/, last accessed 2021/09/27
12. Sensor Community Project. https://sensor.community/en/, last accessed 2021/09/27
13. MQTT: The Standard for IoT Messaging. https://mqtt.org/, last accessed 2021/09/27
14. Node-RED. https://nodered.org/, last accessed 2021/09/27
15. Grafana: The open observability platform. https://grafana.com/, last accessed 2021/09/27
16. Li S, Li W, Cook C, Zhu C, Gao Y (2018) Independently recurrent neural network (INDRNN): building a longer and deeper RNN. In: Proceedings of the IEEE conference on computer vision and pattern recognition, Salt Lake City, UT, USA, pp 5457–5466
17. PROPHET. https://facebook.github.io/prophet/, last accessed 2021/09/27
18. Zhang L, Wen J (2019) A systematic feature selection procedure for short-term data-driven building energy forecasting model development. Energy Build 183:428–442

19. Intelligent Infrared CO_2 Module. https://www.winsen-sensor.com/sensors/co2-sensor/mh-z19b.html, last accessed 2021/09/27
20. DHT22 Sensor. https://www.sparkfun.com/datasheets/Sensors/Temperature/DHT22.pdf, last accessed 2021/09/27
21. PM2.5-PM10 Sensor. https://nettigo.pl/attachments/398, last accessed 2021/09/27
22. LDR. https://www.pcboard.ca/ldr-light-dependent-resistor, last accessed 2021/09/27
23. XBee Zigbee Mesh Kit User Guide. https://www.digi.com/resources/documenta-tion/Digidocs/90001942-13/Default.htm, last accessed 2021/09/27
24. TP4056 1A Standalone Linear Li-lon Battery Charger. https://dlnmh9ip6v2uc.cloud-front.net/datasheets/Prototyping/TP4056.pdf, last accessed 2021/09/27
25. TPL5110 Timer. https://www.ti.com/lit/ds/symlink/tpl5110.pdf, last accessed 2021/09/27
26. DC-DC USB Power Supply Module. https://www.evakw.com/en/power-supply/623-dc-dc-usb-09v-5v-to-5v-boost-step-up-power-supply-module.html, last accessed 2021/09/27
27. Lightweight Low Power Arduino Library. https://www.rocketscream.com/blog/2011/07/04/lightweight-low-power-arduino-library/, last accessed 2021/09/27.

Cloud-Based E-learning: Concepts, and its Beneficial Role During the COVID-19 Dilemma

Rasha Al Bashaireh

Abstract In the epoch of education and emerging technologies, information technology plays a considerable role in the field of education. Cloud computing is one of the most leading emerging paradigms in computing's leverage on education due to its dynamic scalability, high availability, and other valuable characteristics. Traditional E-learning systems have a high infrastructure required to provide concurrent service to various learners. The use of a cloud computing platform offers an effective solution to enhance the quality of education by providing novel methods of learning and teaching which affect both learners and instructors. This paper will introduce why cloud-based E-learning enhances the quality of education by first investigating its concepts, including its architecture and characteristics. A shift from E-learning to cloud-based E-learning is also discussed. Accordingly, the benefits of using cloud-based E-learning are highlighted for the institutions, learners, and instructors. The recent challenges of cloud-based E-learning are also explained, and future work will provide ways to overcome them. The sudden (COVID-19) pandemic has affected general safety, the economy, and education worldwide. As a result, many preventive measures such as lockdowns and social distancing are enforced. Such changes put unprecedented pressure on the education process. To keep up sustained and productive education, educational institutions of all nations switched to online teaching and learning. Hence, the demand for cloud-based E-learning applications has increased to engage learners in the online mode settings. This paper also discusses the impact and benefits of the cloud-based E-learning systems during COVID 19 dilemma.

Keywords E-learning · Cloud computing · Cloud-based E-learning · COVID-19 epidemic

R. Al Bashaireh (✉)
Tafila Technical University, Tafila 66110, Jordan
e-mail: ralbashaireh@ttu.edu.jo

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_43

1 Introduction

Education is an essential aspect of all human beings' lives since education is critical to solve every problem we face. In this era, information technology plays a prominent role in the education sector, providing new ways of teaching outside the classroom, using new emerging technologies to maximize educational outcomes that benefit both students and teachers. Out of the pool of paradigms to gain knowledge via technology, one of the most emerging educational paradigms is E-learning; it is an electronic-based learning procedure developed by interacting with electronically delivered content, related services, and offered support [1].

Recently, E-learning has overwhelmingly been adopted and become an alternative to attend a class in the classic learning paradigm. It effectively integrates learning tools, supporting materials, and prepared content and services to deliver educational content in configurable settings [2]. Table 1 illustrates a brief comparison between the conventional learning and the E-learning approaches, paying attention to the features of learning needs. In E-learning, learners use any computer to learn a certain skill [1]. In addition, other idioms are used to describe this teaching paradigm, like online learning, distributed learning, network learning, and Web-based learning.

Cloud computing has become one of the significant emerging developed areas of research in the past few years. On the authority of the National Institute of Standards and Technology (NIST) in September 2011 [3], cloud computing (CC) is officially defined as a model for enabling ubiquitous, appropriate, on-demand network access to a shared space of configurable computing resources (e.g., storage, applications, servers, networks, and services). Furthermore, these resources can be speedily provisioned and released with the least management effort or service provider interaction. The main goal for CC is to offer efficient access to distant and geographically disseminated resources. Therefore, most popular social networking, email, document

Table 1 Conventional learning versus electronic learning [2]

Categories	Conventional learning	E-learning
Focus on learning	Teacher centered	Student centered
Motivations	Competitions	Cooperation and teamwork
Time and place limits	Limited	No limits
How to respond	Predefined responses	Reconstruction of replies
Content compatibility	Unchanged	Change according to users
Educational prerequisites	Physical space for learners and educational resources	Virtual area for various educational resources
Up-to-date educational resources	Fixed content	Dynamic content
Forms of educational content	Books	Multimedia learning content

sharing, and online gaming sites are hosted on the cloud. Google, Amazon, and IBM are very active in this field.

CC is provided by three different types of services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as services (SaaS) [2]. In IaaS, the associated data and computing infrastructure are provided as a service to the user in the structure of a virtual machine along with related networks and servers. In PaaS, an application development computing platform is provided by cloud providers as a service to the developer [2]. PaaS provides necessary development equipment to developers such as database storage, Web server, operating systems, and programming language editor's space. It opens the door and opportunities for application developers to create their software. It can be run on a cloud platform with no demands to maintain the required software and hardware capabilities. In SaaS, software applications and operating systems are provided to the user by the cloud provider. In this model, the user can utilize the software applications as services that will run on infrastructure organized by the SaaS vendor [2].

CC is becoming a charming technology due to its dynamic and effective employment of resources [4]. E-learning systems have high infrastructure requirements that are necessary to provide concurrent service to many students. Most educational institutions cannot afford such investments and environment; therefore, CC is the finest solution. CC provides the platform to support E-learning. It delivers computing hardware and software resources as a service over the Internet with low cost and fast connectivity, promises scalability, enhanced availability, and cost savings [2].

In the twenty-first century, the whole world faced the most significant challenge called the COVID-19 pandemic. As a result, most nations worldwide imposed rigid restrictions or complete lockdown in schools, colleges, and universities [5]. Here, online education was the only option for higher education (HE) organizations to continue the learning process efficiently during such COVID-19 pandemic emerging crisis. Therefore, the cloud-based E-learning systems were very beneficial for the online teaching–learning processes, providing a broad gamut of services in the educational institutes during the pandemic crisis. Furthermore, cloud-based resources can reinforce the quality of education cost effectively, supporting its sustainability by facilitating the storage capabilities, software, and on-demand infrastructure, benefiting both instructors and learners [5]. More will be discussed regarding the valuable, helpful turn of cloud-based E-learning in the COVID-19 dilemma in Sect. 7.

This paper aims to discuss how CC technology enhanced education. A brief definition of E-learning and a comparison between E-learning and traditional learning is stated first. Then, the shift from E-learning to cloud-based E-learning is discussed, going through its architecture, characteristics, benefits, and challenges. In addition, this paper emphasizes on the valuable role of cloud-based E-learning systems in the COVID-19 dilemma. This paper remainder is arranged as follows: Sect. 2 briefly describes the cloud-based E-learning architecture layers. Section 3 presents the significant concepts of cloud-based E-learning versus conventional E-learning. In addition, the fundamental characteristics of cloud-based E-learning are briefly introduced in Sect. 4. A spotlight on the expected key benefits of using cloud-based E-learning is provided in Sect. 5. Moreover, the challenges of implementing cloud-based E-learning are highlighted in Sect. 6. In addition, the cloud-based E-learning valuable role in the COVID-19 crisis is well discussed in Sect. 7. Finally, the Conclusion and future ideas are summarized in Sect. 8.

2 Cloud-Based E-learning Architecture

Cloud-based E-learning is a type of CC technology in education for E-learning systems that creates the future for E-learning infrastructure [6]. It includes all the needed hardware and software resources used in the traditional E-learning infrastructure. After all these educational materials are virtualized in cloud servers, they can be made available for students, other educational institutions, and businesses in the form of a rent base from cloud vendors [2]. Cloud-based E-learning architecture is divided into five main layers: the infrastructure or hardware resource layer, which performs a dynamic physical host pool [2]; the software resource layer that provides a unified interface for E-learning developers [5]; the resource management layer; the service layer which contains three levels of services (SaaS, PaaS, and IaaS); and finally, the application layer which provides content production, content delivery, education objectives, evaluation component, and management features, as education tools [5].

2.1 Hardware Resource Layer

The hardware resource layer is the most important layer for the whole infrastructure; it supports the higher levels with computing and storage capacity [7]. This layer is composed of information infrastructure such as Internet/Intranet, system software and common hardware. It is also composed of teaching resources which is mainly preserved in the classic teaching model, which then distributed to various domains [6]. This layer comes in the lowest level of cloud service middleware, providing the basic computing power such as the CPU and the physical memory. A virtualization group is created from the physical server, storage, and network via virtualization technology to be triggered by the superior software platform [8]. The congregation of physical hosts is considered dynamic, which means that an unprecedented physical host is appended to enhance and optimize the primary physical computing potency for cloud middleware services. Mention that the user hardly notices any hardware failure in this layer since fault tolerance is allowed in another layer, concluding that hardware resources are not faulted tolerant [2].

2.2 Software Resource Layer

The software resource layer is created and composed with the help of operating systems and middleware. Various types of software resources are incorporated via middleware technology to provide a consolidated interface for software developers, making it easier to embed applications in the cloud, provided for the CC users [9]. This layer basically contains the prepared learning materials and all Web-based services for theory and practical subjects offered by the instructors, easily reached via the Internet. The main elements engaged here are the learners (end users), instructors, and cloud service providers [2].

2.3 Resource Management Layer

The resource management layer is the key to accomplishing loose coupling of software and hardware resources [9]. The management of resource situation, instructor's resource allocation system, user/learner resource system, payment specifics, future requests, and software distribution on various hardware can be achieved by integrating virtualization and CC scheduling strategies [2].

2.4 Service Layer

The service layer is separated into three primary levels of services, namely software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) [7]. In SaaS, CC services are provided for consumers on-demand. As such, cloud consumers can utilize the software on the Internet without purchasing and amendment, where a monthly fee is paid only, which is a different process from the use of traditional software [7]. PaaS is a platform provided for application developers to create and develop their own software, to be delivered later over the Internet. In contrast, the IaaS layer reflects the IaaS infrastructure-related services as the primary lowest layer of the whole network. These layers support the use of a diversity of cloud resources [2].

2.5 Application Layer

The application layer consists of the E-learning application services and tools developed to share integrated learning resources in the CC model, which provides an interactive interface between users by ways of synchronous or asynchronous discussions [2]. Sharing of learning resources includes teacher's course material, teaching

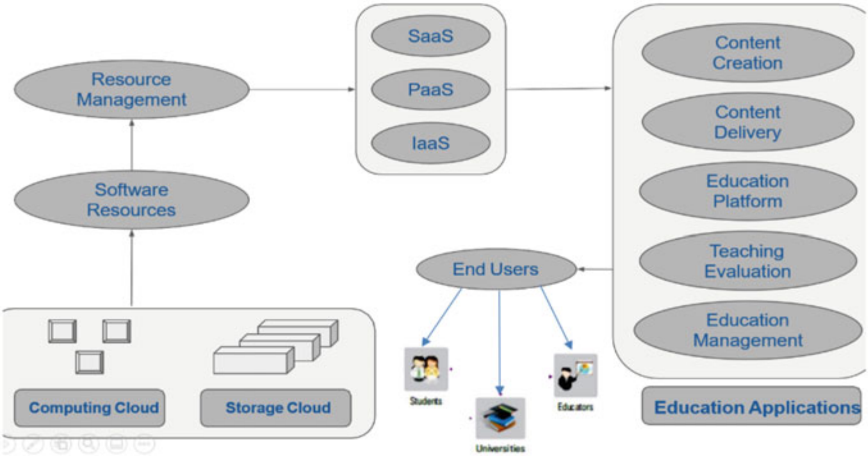


Fig. 1 Architecture of cloud-based E-learning [2, 10]

information resources such as information centers, digital libraries, and multimedia contents [7]. This layer embraces primary learning components, such as content and curriculum creation, learning objectives, content delivery techniques, the assessment component, and finally, the management component [6]. Figure 1 illustrates the services of the CC model related to an education application. As shown, a circular mechanism is proceeding. The computer and the cloud storage dispense the benefits of software and management resource data which is then passed to the three services levels in the CC model. A movement to the next step is later made according to the user's needs once contacting the educational application [10].

3 Concept of Cloud-Based Computing for E-learning

In today's generation, digital education is common place. The resources from which we learn are trending away from tangible items towards Web-based information and resources. The education industry has already seen a shift from classroom-based learning to Web-based. But the promising emerging change now is from standard E-learning to cloud-based E-learning, where it is very appealing for educational institutions compared to traditional E-learning [4].

The concept of cloud-based E-learning is to reside the same fundamentals and resources of traditional E-learning on a cloud-based platform. By doing so, the cloud provider's resources are used instead of an individual educational institution's resources. Despite the institution's decision to adopt IaaS, PaaS, or SaaS, they do not have to eliminate the initial and expensive hardware investment to host their E-learning environment. The cloud provider is thus responsible for the management and maintenance of the hardware resources. Accordingly, the institution's management

Table 2 Electronic-learning versus cloud-based E-learning [2]

Categories	Electronic learning	Cloud-based E-learning
Hardware cost	High	Low
Storage	Fixed capacity	Dynamic capacity
Management	By E-learning professional	By computer technician
Time to implement	Long in comparison	Short in comparison
Processing power	Fixed	Based on demand
Security	More secure in comparison	Less secure in comparison
Overall cost	Initial investment	Pay per use

and maintenance role of the E-learning environment is left to be limited in retrospect. This relationship provides vital benefits for educational institutions, outlined in Sect. 5—learners and instructors as end users also benefit from this highly sophisticated and efficient environment of CC [1]. Educational institutions have many responsibilities that range from housing issues to college food and sports. On the other hand, a cloud provider's primary focus and responsibility are to provide an efficient cloud-computing environment. Undoubtedly, cloud providers can provide computing services much more effectively than educational institutions, which is why the industry is trending toward cloud-based education.

Traditional E-learning and cloud E-learning share a similar primary objective, the education of its users. However, cloud-based E-learning allows this objective to be achieved effectively. In addition to being more effective for end users, cloud-based E-learning is also a more sophisticated option for educational institutions regarding time to implementation, processing power, management, and cost [2]. Table 2 outlines some general distinctions between E-learning and cloud-based E-learning in respect to hardware cost, storage, management, time to implement, processing power, security, and overall cost. In all the categories except security, cloud-based E-learning is the breadwinner.

4 Cloud-Based E-learning Characteristics

Cloud-based E-learning environments share essential characteristics, which are broken down into the following six categories: availability, communication, collaborative environment, resource pooling and elasticity, data, and measured services. Described below.

4.1 Availability

One of the most important characteristics a cloud-based E-learning environment should retain is high availability. Learners and instructors need stable connectivity and on-demand access to educational resources maintained in the cloud. Access should also be achievable from a multitude of devices and platforms. Therefore, high-performance computing power and large storage capabilities are well utilized by cloud providers to efficiently provide resources [7]. Moreover, in terms of broad network access, high bandwidth should also be provided to ensure cloud servers' connection efficiency [2].

4.2 Communication

The cloud environment facilitates communication between students and instructors via direct one-to-one communication like e-mail, webinars, or live sessions [11] and indirect contact such as uploading assignments and course material, providing grades, and creating announcements. To ensure these services, cloud providers should maintain the characteristics of availability, elasticity, and data access. Moreover, communication can be enhanced by guaranteeing fault tolerance in the cloud environment. Thus, cloud providers must have a pre-devised methodology for handling unexpected failures, such as detecting the node with failure and then diverting to another node [7]. This results in an available and reliable system for the end users.

4.3 Collaborative Environment

One of the major distinctions between non-cloud and cloud E-learning is the access of data and resources, where cloud-based educational systems encourage a collaborative environment. Therefore, cloud providers should manage a flow of users' requests attempting to access the same resources and data simultaneously. This is important regarding sharing content for project-based learning settings. Moreover, cloud-based educational services, such as Moodle, improve collaboration between teachers and students [11]. The teachers create and distribute content, and students can access materials despite time and space conditions.

4.4 Resource Pooling and Elasticity

Cloud provider resources and pooling of computing services are located in various areas, on different platforms, and running other software. However, to the end user, the provider should ensure a seamless environment. In instances of SaaS, the provider should enable multiple access levels, and multitenancy, where users are isolated from each other, and resources are assigned to them in response to their demands [2]. For instance, in education, the educational institutions have many faculties and students that need access to cloud resources concurrently, the cloud provider should ensure resources are dynamically assigned and reassigned according to user demand. This creates rapid elasticity, where the virtual cloud can control the allocated resources rapidly and automatically respond to specific requirements, such as expanding through the examination time and reducing during vacations.

4.5 Data

Cloud-based data providers should guarantee data availability, reliability, and security for their user's data. Furthermore, since data storage in the cloud is an essential part of the E-learning settings, cloud providers must provide redundancy methods to back up data in their servers. Thus, no loss of data happens in case of a user's device failure.

4.6 Measured Services

Students use educational resources provided by the cloud differently. Thus, cloud providers must monitor the provisioning of services. This will aid in determining the amount to bill the institution, where a level of transparency is provided for the providers and users regarding the used services by monitoring and controlling the resource usage. Typically cloud providers charge on a pay-per-use basis [3].

5 Cloud-Based E-learning Benefits

Cloud-based E-learning has many valuable benefits, described in terms of benefits for educational institutions, learners, and instructors as follows:

5.1 Benefits for Educational Institutions

Educational institution benefit is summarized as decreased costs, enhanced storage capacity, latest versions and software updates, and device independence. In decreased costs, E-learning users can run the applications from the cloud through their PC, mobile phones, tablet PC having a minimum configuration with Internet connectivity. No need for a high-end configured computers to run E-learning applications anymore. The institutions only require systems with the least possible memory, low processing capability, and less storage to run a Web application established on the cloud. Moreover, the institutions have to pay per use, and for space they need. While in enhanced storage capacity, cloud provides unlimited storage capacity as compared to other servers; usually, the user was restricted to the storage of a single personal computer or server on a network [12]. CC will allow for the institutions to upload and save a vast amount of data without any concern [2].

In latest versions and software update, the institutions do not have to worry about the software versions because the CC always updates the software and have the latest version; therefore, there is no risk of having an outdated version of software on the computer device [12]. Concerning device independence, users no longer need to tie to a single computer or network; their existing applications and documents will be provided via the cloud [13].

5.2 Benefits for Learners

The general benefits for learners and students are summarized as worldwide access to resources, easier collaboration for team-based projects, increased computing power, and online course. In the worldwide access to resources, students can require documents on the cloud geographically. Therefore, the students can access any resources they need from anywhere. While in easier collaboration for team-based projects, the learners can collaborate easily to perform the different tasks doing a particular project. In increased computing power, CC is beneficial for students' research, project, and other activities because it supplies many processing powers [2]. Also, more resource-consuming jobs may be accomplished with a single personal computer [12].

In an online course, students can continue their classes from anywhere in the world. For example, students studying abroad can pursue their classes and take their exams online when they travel back home in the summer semester. Also, they can get feedback about the courses from instructors and send their projects and assignments online to their teachers.

5.3 Benefits for Instructors

Instructors benefited from the cloud-based E-learning technology in many teaching-related tasks such as providing better content resources for learners, Facilitating feedback submission, increased data reliability, better interaction, and communication with learners. CC helps teachers offer better digital resources for students like video, DOC, PPT, and PDF files for book references. The feedback submission feature is also facilitated using CC; students can submit their assignments online, and the teacher can accordingly give feedback. This saves time for both instructors and students. Concerning the increased data reliability, it means that if the teachers' computers crash for any reason, they still can access all their data since it resided in the cloud [13]. The data reliability eliminates the necessity to backup documents and possession of portable hard drives [12]. In better interaction and communication with learners, the teachers can communicate with their students rapidly in a convenient way online. For instance, to the time of 2021 era, the professors at Tafila Technical University used Moodle to communicate with their students because it is the easiest available way for online interaction since students can receive a notification email to know there is something sent to them.

6 Cloud-Based E-learning Challenges

Nowadays, most educational institutions have established portals to provide an E-learning environment to overcome the traditional learning approach or support online long-distance learning. However, there are apparent challenges in implementing CC to E-learning technology despite all the valuable benefits of cloud-based E-learning systems. These challenges are related to well-known technical issues such as network connection, reliability, portability, security, and privacy. Since the entire idea of cloud service depends on a network, a constant Internet connection is required to pursue cloud functionalities and accomplish users' tasks. A cloud connection failure can cause loss of users' unsaved data, efforts, time, and accomplished work [13]. Thus, it is impossible to use CC in areas with a loss of Internet connection [12].

Furthermore, reliability is a severe concern for the majority of educational institutions that adopt the CC systems. Since the cloud servers also experience slowdowns and downtimes, simultaneously, consumers depend on the cloud service provider [14]. While efficient resources such as bug fixes and technical support are hardly offered by some cloud service providers, especially from developed countries [15]. Regarding the security issue, it is an essential aspect when dealing with E-learning systems and materials. Most educational institutions have a sense of insecurity about storing their data and information on CC systems that they do not fully control [13]. Thus, SaaS providers must provide a high-security level to guarantee subscribers' trust since their data is held on various providers to be securely integrated and utilized [2].

In general, and due to the nature of CC, exploring the privacy issue is complex. However, tremendous challenges regarding the privacy of CC are noticed, especially for data, such as access, storage, retention, audit, and monitoring, besides the breaches and debates of many related legal systems [15]. One of the last challenges to mention here is the portability issue; since many students and instructors complete their work at home, they might face proprietary interfaces limits when trying to provide systems back in-house or joining another cloud provider [13]. More challenges will be investigated as future work for this paper, especially those related to the use of cloud-based E-learning capabilities in the COVID-19 pandemic.

7 Beneficial and Valuable Role of Cloud-Based E-learning Platforms in the COVID-19 Dilemma

Through the sudden storm of the COVID-19 pandemic crisis, recent technology has played a crucial role as a lifesaver. Accordingly, the World Wide Web was the most predominant medium to pursue the teaching–learning process during the lockdown. Here, the power of the E-learning systems was revealed to be a significant tool for instructors in the entire globe to continue the education process [16]. University faculty, schoolteachers, and courses instructors utilized well-developed E-learning platforms to share class materials and lectures in diverse forms (Word document, PPTs, PDFs, slideshows, and audio-visual videos) through some leading online educational Web cloud-based applications, such as Zoom, Microsoft Teams, and G-suite cloud meeting. [16]. These well-known educational applications provided many valuable features for free to the educational institutes. Such features involve curriculum management features, time-table automation and organizing, homework preparation, direct messaging, and grading features [16]. Hence, a considerable growth of their users is noticed. According to a recent report, Microsoft Team consumers were about 750 on March 10; then by the beginning of the COVID-19 crisis, around March 24, they reached up to 138,698 [17].

Due to the ongoing COVID-19 crisis, the needs of today's learners can be fulfilled by the use of cloud-based E-learning systems that have been proven very beneficial for the online teaching–learning processes during such crisis due to many reasons [16]. The adoption of such applications was mandatorily needed by educational organizations, in general, and by higher educational organizations, in specific. The E-learning cloud-based systems follow a new scheme of online data storage, processing, and management as a substitute for conventional servers. This new model provides easy online access to enormous computing capabilities. Such cloud-based systems can deliver their 24 × 7 services in scalable, easily attainable, reliable, safe ways [5]. Owing to the emerging benefits of cloud-based E-learning, they can provide a broad gamut of services for the education process in educational institutes. Furthermore, cloud-based resources can reinforce the quality of education cost effectively, preserving its sustainability, benefiting the instructors and the learners [5].

The COVID settings made teachers change and improve their pedagogical approaches to suit the online courses delivery process [16]. Here, their creation of online course materials was delivered in many surprising, innovative ways by the support of cloud-based systems, motivating students in the learning process. As stated by a survey result done in [11], some faculty members benefited positively from the cloud-based E-learning systems. They mentioned that it changed their way of teaching by reaching out to their students more efficiently and effectively through chat groups, live video meetings during this pandemic [11].

Furthermore, either university or school students positively impacted their learning process during the COVID dilemma using such cloud-based E-learning systems. They can acquisition an immense amount of information at their own convenience despite time and space conditions. Furthermore, Webinars and direct live communications with their instructors are facilitated via such cloud-based educational applications. This offers a straightforward, smooth, gradual, convenient approach for self-learning [16]. For instance, Sc Edu-page cloud-based school management system portal has been excessively adopted at 150,000 schools covering 173 countries worldwide due to its free access and user-friendly functionalities [18]. Moreover, students can save a significant amount of money since traditional courses are considered more expensive than online ones. Besides, the COVID situation and the emerging E-learning technology allowed learners to earn their livelihood and enhance their qualifications, accommodating both learnings and earning money and life. Lastly, E-learning enabled learners in the COVID-19 hard times to access and share materials smoothly, either by directly uploading to prepared cloud storage or sharing via a social network, thus improving the learners' and students' collaboration, especially in project-based learning settings. In addition, learning management system (LMS) is also a kind of cloud-based educational service, such as Moodle, used by both teachers and students effectively during the COVID dilemma to achieve the learning objectives [11]. The teachers create and distribute content and evaluate students' performance. In contrast, students can access materials freely despite time and space conditions. Also, they can participate in the live examination sessions. LMS can facilitate the following activities: Enrolling students online for Web-based actions; scheduling contents; deliver virtual lectures; tracking students' performance; communication by e-mail, webinars, or live sessions [11]. Furthermore, such LMS can help in collecting feedback and data for overseeing the educational procedures in a particular educational institution.

8 Conclusion and Future Work

Educational institutions are and have been trending towards using Internet-based technology to provide educational services. They faced many challenges when implementing non-cloud-based E-learning systems, including initial hardware cost and continued overhead cost for managing and maintaining. Cloud-based services offer a more effective solution for universities to provide an E-learning environment for their faculty and students. Educational resources can be accessed from any device despite anywhere, anytime conditions. Cloud-based learning systems are a new attractive E-learning paradigm for providing E-learning services. They require a low cost of hardware and software, have flexible deployment, and require less onsite maintenance. Thus, educational institutions no longer pay for infrastructure because the cloud service provider provides it. The sudden blast of the COVID-19 virus, especially in educational organizations, won't be handled effectively without E-learning systems. This worldwide COVID-19 pandemic has manifested the enormous value of E-learning globally. Therefore, it was worth it in this paper to focus on cloud-based E-learning applications and their beneficial role in the COVID-19 pandemic to all institutions, instructors, and learners. With all the benefits CC provides for the

E-learning environment, some challenges need to be addressed in future work, especially data privacy challenges, such as access, storage, audit, and monitoring. As time progresses, solutions for the recent challenges will be developed just in time for new challenges to arise, especially with all the emerging problems due to the extensive use of cloud-based E-learning platforms during the COVID-19 pandemic. However, the educational benefits significantly outweigh any negatives stemming from cloud-based E-learning. In the future, more challenges will also be addressed, especially those related to the use of cloud-based E-learning capabilities in the COVID-19 pandemic. In addition, the future of this study aims to investigate more about the cloud-based E-learning architecture. It also aims to propose a new architecture model to enhance the educational institutions' E-learning cloud-based application services that can suffer from the momentum of use, especially in such worldwide crises like COVID-19.

References

1. Bosamia M, Patel A (2016) An overview of cloud computing for E-learning with its key benefits. Int J Inf Sci Tech 6:1–10
2. Bibi G, Sumra IA (2017) A comprehensive survey on E-learning system in cloud computing environment. Eng Sci Technol Int Res J 1(1):43–50
3. Mell P, Grance T (2011) The NIST definition of cloud computing—SP 800-145. NIST Spec Publ 145:7
4. Ghazizadeh A (2012) Cloud computing benefits and architecture in E-learning. In: Proceedings 2012 17th IEEE international conference on wireless, mobile and Ubiquitous technology in education, WMUTE 2012, pp 199–201. https://doi.org/10.1109/WMUTE.2012.46
5. Bhardwaj AK, Garg L, Garg A, Gajpal Y (2020) E-learning during COVID-19 outbreak: cloud computing adoption in Indian Public Universities. Comput, Mater Continua 66:2471–2492
6. Masud MAH, Huang X (2012) An E-learning system architecture based on cloud computing. System 10(11):255–259
7. Selviandro N, Hasibuan ZA (2013) Cloud-based E-learning: a proposed model and benefits by using E-learning based on cloud computing for educational institution. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7804 LNCS, pp 192–201
8. Paul C, Santhi R (2014) A study of E-learning in cloud computing. Int J Adv Res Comput Sci Softw Eng 4(4):729–734
9. Riahi G (2015) E-learning systems based on cloud computing: a review. Procedia Comput Sci 62:352–359
10. Dhull K (2013) Cloud computing efficiency metrics for enhanced E-learning implementation model based on view controller design pattern paradigm. Int J Inf Futuristic Res (IJIFR) 1(4):79–87
11. Ziaul Hoq M (2020) E-learning during the period of pandemic (COVID-19) in the Kingdom of Saudi Arabia: an empirical study. Am J Educ Res 8:457–464
12. Karim F, Goodwin R (2013) Using cloud computing in E-learning systems. Int J Adv Res Comput Sci Technol (IJARCST) 1:65–69
13. Leloglu E, Ayav T, Aslan BG (2013) A review of cloud deployment models for E-learning systems. Proc Int Conf Dependable Syst Netw. https://doi.org/10.1109/DSN.2013.6575331
14. Viswanath DK, Kusuma S, Gupta SK (2012) Cloud computing issues and benefits in modern education. Glob J Comput Sci Technol Distrib 12:15–19

15. Alghali M, Najwa HMA, Roesnita I (2014) Challenges and benefits of implementing cloud based E-learning in developing countries. Proc Soc Sci Res ICSSR 2014:1–9
16. Soni VD (2020) Global impact of E-learning during COVID 19. SSRN Electron J. https://doi.org/10.2139/ssrn.3630073
17. Reimers FM, Schleicher A (2020) A framework to guide an education response to the COVID-19 pandemic of 2020. Rev Educ Res 66:227–268
18. Edu EDUPAGE. https://www.edupage.org/, last accessed 2021/10/20

Packet Replays Prevention Protocol for Secure B5G Networks

Vincent Omollo Nyangaresi, Junchao Ma, Mustafa A. Al Sibahee, and Zaid Ameen Abduljabbar

Abstract The beyond 5G networks (B5G) are characterized by high throughputs at extremely low latencies and better energy consumptions. This has seen them being deployed as the backbone of numerous Internet of Things (IoT) application domains such as smart homes, smart cities and in intelligent transport systems. Massive and private data flows in these ultra-dense networks and hence the need to protect them. As such, the Third-Generation Partnership Project (3GPP) has defined Authentication and Key Agreement (AKA) protocols for secure signaling and packet exchanges in these networks. However, these AKA protocols are susceptible to numerous attacks, such as impersonation and packet replays. This has seen the development of numerous schemes based on techniques such as public key cryptography, biometrics, group signatures and blockchain. Unfortunately, these schemes fail to offer the required levels of security and privacy protection at low execution time, energy and bandwidths. In this paper, a protocol is developed that leverages on the message authentication codes , symmetric cryptography and elliptic curve cryptography. It is

V. O. Nyangaresi (✉)
Faculty of Biological & Physical Sciences, Tom Mboya University College, Homabay, Kenya
e-mail: vnyangaresi@tmuc.ac.ke

J. Ma · M. A. Al Sibahee
College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
e-mail: majunchao@sztu.edu.cn

M. A. Al Sibahee
e-mail: mustafa@sztu.edu.cn; mustafa.alsibahee@iuc.edu.iq

M. A. Al Sibahee
Computer Technology Engineering Department, Iraq University College, Basrah, Iraq

Z. A. Abduljabbar
Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
e-mail: zaid.ameen@uobasrah.edu.iq

Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen, China

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_44

shown that the proposed protocol is secure under the Dolev–Yao model. In terms of performance, it exhibited the lowest execution time and has the lowest bandwidth requirements.

Keywords Authentication · Cryptography · Dolev–Yao · ECC · Key agreement · Privacy · Security

1 Introduction

The Fifth Generation (5G) and beyond networks (B5G) offer massive connectivity at extremely low latencies and energies, high reliability and with high throughputs. These features render these networks applicable to various Internet of Things (IoT) scenarios such as smart health, smart homes and smart grids [1]. Autonomous driving, virtual reality, remote surgery, device-to-device communication and teleportation are other application domains that depend on B5G networks. Unfortunately, the support of many applications using diverse connection technologies exposes the B5G networks to numerous security and privacy attacks [2]. In addition, it makes it cumbersome to distribute and manage public keys and certificate that are typically deployed for authentication [3]. As pointed out in [4], the heterogeneous nature of these networks implies numerous distributed servers and small cells and hence massive data exchanges among the connected devices. Insecure transmission of messages in these networks has severe security and privacy issues [5]. This can be attributed to the ease with which a single compromised device will propagate malware among all the connected devices as well as to the core network [6]. As explained in [7], attackers can easily eavesdrop the traffic channels as well as insert bogus messages in the communication network.

One possible solution to the security and privacy issues in B5G networks is mutual authentication and key agreement that should precede any data exchanges [8, 9]. As such, the Third-Generation Partnership Project (3GPP) has introduced Authentication and Key Agreement (AKA) protocols in these networks. Apart from AKA protocols, authorization services are critical in B5G as they serve to thwart some of the security and privacy issues. Unfortunately, the conventional AKA protocols are inadequate in the management of a myriad of devices such as those supported by B5G networks [10]. Worse still, these protocols are vulnerable to attacks such as Denial of Services (DoS), impersonation and Man-in-the-Middle (MitM) [11].

Consequently, the provisioning of security while at the same time upholding the required level of Quality of Service (QoS) requires novel security architectures that offer flexible privacy and security [12]. These new security models will support advanced B5G technologies that are envisioned to offer convenient and ubiquitous computing [13]. For instance, in 5G-based wireless sensor networks (WSNs) and IoT, massive smart devices and sensors collect high volumes of private data. Although the collected information is deployed for intelligent decision making that provide comfort and convenience, it increases attack surfaces from which adversaries may invade the networked smart systems [8].

Although massive machine-type communications (mMTCs) coupled with ultra-reliable and low-latency communications (URLLC) offer device ultra-densification, low latencies and energy efficiency, the adoption of small cells in B5G networks results in frequent handovers and hence frequent authentications. Consequently, there is increased latency which contracts the B5G goals. This calls for fast and efficient authentication protocols to offer the much needed scalability [14]. The computing power of the devices in these networks, such as sensors and actuators, is very limited [15]. As such, the authentication protocols in B5G are required to be lightweight so as to consume the least energy and bandwidth [5]. In this paper, the following contributions are made:

I. A protocol that leverages on the message authentication codes, symmetric cryptography and elliptic curve cryptography is developed for B5G authentications

II. It is shown that the proposed protocol is secure under all the Dolev–Yao model security assumptions

III. Performance evaluation of the proposed protocol shows that it has the least execution time at the lowest bandwidth requirements

IV. It is shown that II and III above endear the proposed protocol applicable to B5G networks.

The rest of this research article is structured as follows: Sect. 2 discusses related work, while Sect. 3 highlights the system model of the proposed protocol. On the other hand, Sect. 4 presents and discusses the simulation results, while Sect. 5 concludes the paper and gives future directions.

2 Related Work

Numerous protocols have been presented in literature to offer protection to the traffic and signaling data exchanged over B5G networks. For instance, authors in [16] have introduced an authentication scheme to thwart active attacks. However, the AKA in [16] is still susceptible to impersonation, packet replays, DoS and MitM attacks. On the other hand, the authentication scheme presented in [10] has scalability issues, while the scheme in [17] has high computation and communication overheads. Authors in [18] and [19] have developed blockchain-based authentication frameworks for increased trust levels among the communicating entities. Although the schemes in [18] and [19] offer integrity protection and intrusion prevention, they have high computation and storage requirements due to deployment of blockchains [20] which is not ideal for B5G-supported IoT communications [21].

The identity-based authentication scheme presented in [22] uses secret keys to validate the user equipment (UE) to the home network (HN). However, this protocol lacks the registration phase and is still vulnerable to impersonation attacks. Authors in [23] have presented a privacy-preserving authentication technique. Unfortunately, the scheme in [23] is susceptible to de-synchronization attacks. On the other hand, the public key cryptography-based protocol in [24] has key escrow issues. In addition, it potentially results in high communication and computation overheads [25]. Authors in [26] have introduced two anonymous AKA protocols, but these protocols fail to offer user privacy. Similarly, two group key authentication protocols have been presented in [27] for privacy preservation. However, the schemes in [27] have high computation costs and are susceptible to MitM attacks should one of the group members turn out to be malicious [28].

A Diffie–Hellman-based authentication scheme is presented in [29] to offer protection against linkability and MitM attacks. However, the deployment of public keys during the authentication phase may lead to increased latencies [25]. In addition, this protocol is vulnerable to de-synchronization attacks and has high communication overheads. A three-factor authentication scheme is introduced in [30]. Unfortunately, this protocol does not address biometric noise [31]. Similarly, the scheme in [32] cannot uphold forward key secrecy and is not robust against privileged insider attacks. Authors in [33] have developed a protocol to prevent distributed DoS attacks. However, this technique cannot scale well with increased communication sessions. On the other hand, the authentication scheme in [34] fails to validate packet headers and is susceptible to flooding attacks.

3 System Model

In the proposed protocol, the 5G core network comprises various functions instead of physical entities. Specifically, network function virtualization (NFV) and software-defined networking (SDN) are integrated with the packet core network entities such as the Access and Mobility Function (AMF), User Plane Function (UPF), Unified Data Management (UDM), Policy Control Function (PCF), Session Management Function (SMF), Authentication Server Function (AUSF), Network Repository Function (NRF), Application Function (AF), Network Slice Selection Function (NSSF) and Network Exposure Function (NEF). As shown in Fig. 1, the 5G network interconnects various communication technologies such as IoT, cloud computing, Internet, relay nodes, multiple-input and multiple-output (MIMO) and mobile relay nodes (MRNs) among others. In this environment, security and privacy are major issues as vulnerabilities in one network component can compromise the entire system. Strong mutual authentication followed by session key agreement is the first step toward securing the B5G networks.

The proposed protocol involved three parties, which included the user equipment (UE), source gNB and target gNB (TgNB). The proposed authentication and key agreement protocol is executed whenever any of the network entities such as UEs or smart devices attempts to request for any B5G services.

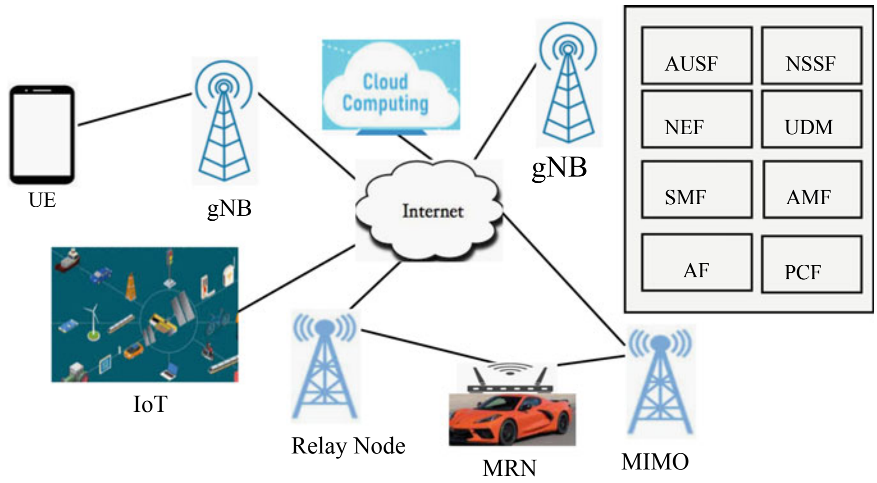


Fig. 1 Network architecture

As already pointed out, the proposed protocol deployed message authentication codes, symmetric cryptography and elliptic curve cryptography. The ECC mathematical formulations and hardness problems deployed in this algorithm are the same as those in [28]. Table 1 presents the symbols used in this article together with their brief descriptions.

The requested service in this case is the handover from the source gNB toward the target gNB. It is assumed that the UE had executed the same authentication and key agreement procedures before connecting to the source gNB. As such, only the authentication to the target gNB is considered in this protocol. The proposed protocol was executed in three major phases, which comprised of the parameter setting phase, mutual authentication and finally the key agreement phase. These phases are discussed in the subsections that follow.

3.1 Parameter Setting Phase

This phase consisted of the following three steps:

Step 1: The TgNB selects point Q of order N over E and generates both $\mathbb{H}$ and $\mathbb{C} = \mathbb{H}.Q$. This is followed by the selection of h(.) before buffering $\mathbb{H}$ in its repository.

Step 2: Generate UE_{ID} for the ith UE together with both $\mathfrak{H}$ and $\mathfrak{R}$. Next, the TgNB derives $\mathscr{B} = h(UE_{ID})$ and $\Psi = Q(\mathscr{B} + \mathbb{H})$. Since $\mathbb{C} = \mathbb{H}.Q$, we have: $\Psi = Q\mathscr{B} + \mathbb{C}$.

Table 1 Symbols and their descriptions

Symbol	Description
E	Elliptic curve
$\mathbb{H}$	High entropy master key
$\mathbb{C}$	TgNB public key
h(.)	One-way hashing operation
Q	A point on E of order *N*
F_Q	Finite field of order *N*
UE_{ID}	UE identity
$\mathfrak{H}$	UE's secret token
$\mathfrak{R}$	$\mathfrak{H}$'s identity
Ψ	UE's public key
ζ	UE private key
χ	Group of Q points on E
T_{ID}	Tracking area identity
||	Concatenation operation
$\oplus$	XOR operation
Ri	Random numbers
$\acute{\Gamma}$i	Timestamps
$E_{\mathfrak{H}}$	Encryption using $\mathfrak{H}$
$D_{\mathfrak{H}}$	Decryption using $\mathfrak{H}$
$\mathfrak{I}_i$	Pseudo-random numbers
A_{Req}	UE authentication request
A_{Res}	TgNB authentication response
$\Delta\acute{\Gamma}$	Transmission latency
$\phi_{T,}$ ϕ_U	TgNB and UE session keys respectively

Step 3: Using $\mathbb{H}$, the TgNB computes UE's private key $\zeta = Q(\mathbb{H} + \mathcal{B})^{-1} \in G$. Afterward, TgNB buffers all computed parameters before sending M = {h(.), E, N, $\mathbb{C}$, Q, F_Q, $\mathfrak{H}$, $\mathfrak{R}$, $\mathscr{B}$,ζ} to UE through some secure channel.

3.2 Authentication and Key Agreement Phase

These two phases involved the following five major steps:

Step 1: The UE selects $R_1 \in Z_N^*$ and derives Ï = R_1.Q and Ÿ = $R_1.\zeta$ before determining current timestamp $\acute{\Gamma}_1$. It then proceeds to compute security parameters $A_1 = h(UE_{ID}||T_{ID}||\ddot{I}||\ddot{Y}||\acute{\Gamma}_1)$ and $A_2 = E_{\mathfrak{H}}(UE_{ID}, T_{ID,}\ \acute{\Gamma}_1)$.

Step 2: To uphold integrity for the exchanged packets, the UE derives $B_1 = MAC_{A_1}(UE_{ID}, \acute{\Gamma}_1, \ddot{I})$. Next, it generates $\mathfrak{I}_1$ that it uses to derive $\mathbb{Z}$ =

$h(T_{ID}||\Im_1) \oplus (\Re||\acute{\Gamma}_1)$ before sending authentication request $A_{Req} = \{\mathbb{Z}, A_{2,} \ddot{I}, B_1, \Im_1, \acute{\Gamma}_1\}$ to the TgNB.

Step 3: Upon receipt of A_{Req}, TgNB determines $\acute{\Gamma}_2$ and checks whether $(\acute{\Gamma}_2 - \acute{\Gamma}_1) \leq \Delta\acute{\Gamma}$. If this condition does not hold, the authentication process is aborted. However, if this condition is true, it computes $h(T_{ID}||\Im_1)$ and retrieves $\Re$, $\mathfrak{H}$ and UE_{ID} from its repository. It then executes decryption $D_{\mathfrak{H}}(A_2)$ to yield $UE_{ID}{}^*$, $T_{ID}{}^*$ and $\acute{\Gamma}_1{}^*$. Next, it verifies whether $UE_{ID}{}^* = UE_{ID}$, $T_{ID}{}^* = T_{ID}$ and $\acute{\Gamma}_1{}^* = \acute{\Gamma}_1$. On condition that these validations are unsuccessful, the authentication process is aborted. However, these checks are successful, the TgNB derives $\mathscr{B}^* = h(UE_{ID})$, $\ddot{Y}^* = \ddot{I}(\mathbb{H} + \mathcal{B}^*)^{-1}$, $A_1{}^* = h(UE_{ID}||T_{ID}||\ddot{I}||\ddot{Y}^*||\acute{\Gamma}_1)$ and $B_1{}^* = MAC_{A_1^*}(UE_{ID}{}^*, \acute{\Gamma}_1{}^*, \ddot{I})$. It then verifies whether $B_1{}^* = B_1$ such that if this condition does not hold, the authentication process is aborted, otherwise it proceeds to the next step as shown in Fig. 2.

Step 4: The TgNB chooses random number $R_2 \in Z_N^*$ that is deployed to derive $C_1 = R_2.Q$, $C_2 = R_2.\ddot{I}$, $A_3 = E_{\mathfrak{H}}(UE_{ID}, T_{ID,} \acute{\Gamma}_2)$, $B_2 = MAC_{A_1^*}((T_{ID}, \acute{\Gamma}_2, C_1)$. This is followed by the computation of session key $\phi_T = h(UE_{ID}||T_{ID}||\ddot{I}||C_1||C_2)$. Next, it generates $\Im_2$ that is employed to derive security parameter $D_1 = h(T_{ID}||\Im_2||) \oplus (\Re||\acute{\Gamma}_2)$. Finally, TgNB sends authentication response $A_{Res} = \{D_1, C_1, A_3, B_2, \Im_2, \acute{\Gamma}_2\}$ back to the UE.

Step 5: On receiving $A_{Res,}$ the UE determines current timestamp $\acute{\Gamma}_3$ used to check whether $(\acute{\Gamma}_3 - \acute{\Gamma}_2) \leq \Delta\acute{\Gamma}$. Provided that this freshness check returns false, the authentication process is aborted, otherwise the UE retrieves $\Re$ from its memory before executing $D_{\mathfrak{H}}(A_3)$ to obtain $UE_{ID}{}^*$, $T_{ID}{}^*$ and $\acute{\Gamma}_2{}^*$. Afterward, the UE verifies whether $T_{ID}{}^* = T_{ID}$ and $\acute{\Gamma}_2{}^* = \acute{\Gamma}_2$. If the verification results are negative, the authentication session is aborted, otherwise it derives $B_2{}^* = MAC_{A_1}((T_{ID}, \acute{\Gamma}_2{}^*, C_1)$. This is followed by the verification of whether $B_2{}^* = B_2$ and if the result is negative, the authentication process is aborted. However, if the result is positive the UE proceeds to derive $D_2 = R_1.C_1$ and compute session key $\phi_U = h(UE_{ID}||T_{ID}||\ddot{I}||C_1||D_2)$ for traffic protection. Consequently, the communication channel between the UE and TgNB is now fully authenticated, and they can commence payload exchanges.

4 Results and Discussion

This section presents the security evaluation as well as the performance evaluation of the proposed protocol as discussed below.

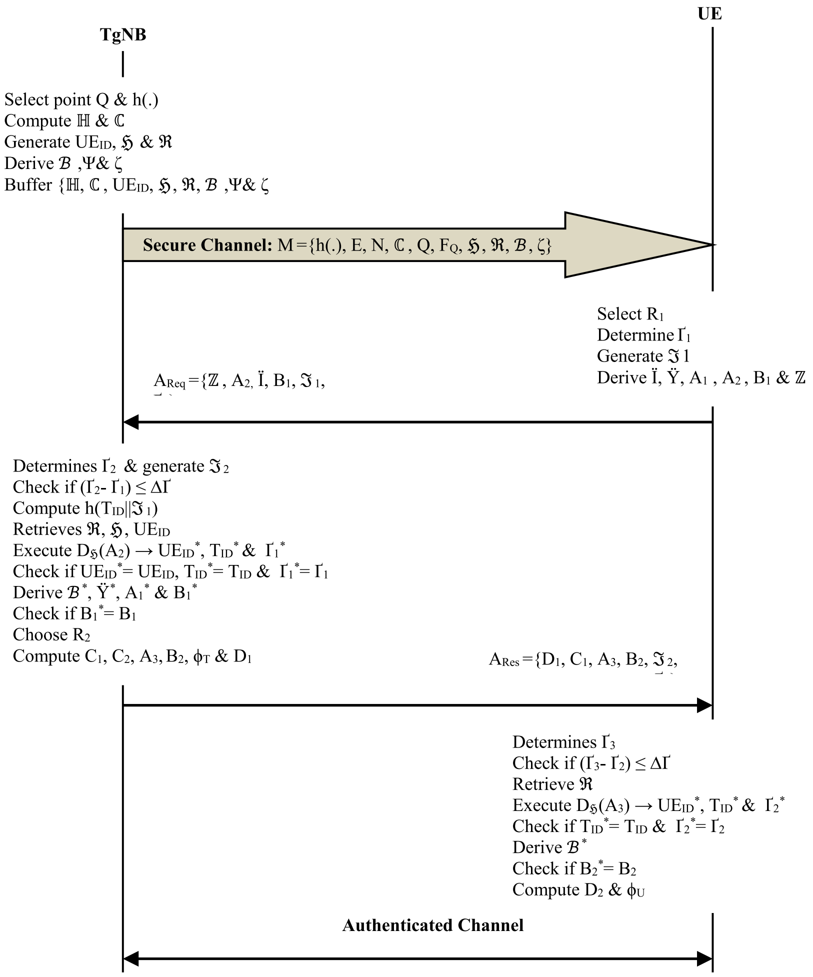


Fig. 2 Message flows in the proposed protocol

4.1 Security Evaluation

In this section, it is shown that the proposed protocol is secure under the Dolev–Yao model assumptions as discussed in [15]. The robustness of the proposed protocol is based on the computational complexities of hashing algorithms, encryption protocols and EC discrete logarithmic problem (ECDLP) elaborated in [28].

Proposition 1 *The proposed protocol is resilient against packet replays.*

Proof Suppose that an adversary eavesdrops the communication channel during the authentication and key agreement phase and manages to capture $\{\mathbb{Z}$, $A_{2,}$ Ï, B_1, $\Im_1$,

$Ґ_1$} sent from the UE to the TgNB. The aim is then is to retransmit this message at time $Ґ^A$: { $\mathbb{Z}$, A_2, $Ï$, B_1, $\Im_1{}^A$, $Ґ_1{}^A$} → TgNB. However, in the proposed protocol, freshness check is executed for all the exchanged messages and hence this replayed message will fail the ($Ґ_2$- $Ґ_1{}^A$) $\leq \Delta Ґ$ check at the TgNB. In addition, an attacker needs a valid UE identity UE_{ID} and tracking area identity T_{ID} to derive a legitimate $A_2 = E_{\mathfrak{H}}(UE_{ID}, T_{ID}, Ґ_1)$. Since the attacker has no knowledge of encryption key $\mathfrak{H}$, the derivation of valid A_2 is infeasible and this attack flops. Suppose now that an attacker is interested in going through the $B_1{}^* = B_1$ verification process. This requires correct computation of $A_1 = h(UE_{ID}||T_{ID}||Ï||Ÿ||Ґ_1)$ deployed to derive $B_1 = MAC_{A_1}(UE_{ID}, Ґ_1, Ï)$. However, based on the ECDLP axioms, getting R_1 used to compute $Ÿ = R_1.\zeta$ is a computationally hard problem. In addition, changing timestamp $Ґ_1$ in $A_2 = E_{\mathfrak{H}}(UE_{ID}, T_{ID}, Ґ_1)$ requires knowledge of encryption key $\mathfrak{H}$ which is only known to the TgNB and UE.

Suppose now that the attacker wants to replay message {D_1, C_1, A_3, B_2, $\Im_2$, $Ґ_2$} sent from the TgNB toward the UE. This requires the eavesdropping of this message over the communication channels, after which an attempt is made to retransmit it at time $Ґ^A$: {D_1, C_1, A_3, B_2, $\Im_1{}^A$, $Ґ_1{}^A$} → UE. However, during freshness check ($Ґ_3$- $Ґ_1{}^A$) $\leq \Delta Ґ$, this bogus message will be detected. Further, during $B_2{}^* = B_2$ verification, an adversary needs to derive valid $B_2{}^* = MAC_{A_1}((T_{ID}, Ґ_2{}^*, C_1)$, which requires knowledge of R_2 to derive legitimate $C_1 = R_2.Q$. This represents a computationally hard problem in accordance with ECDLP. Moreover, the timestamp $Ґ_2$ in $A_3 = E_{\mathfrak{H}}(UE_{ID}, T_{ID}, Ґ_2)$ cannot be changed since encryption key $\mathfrak{H}$ is not known to the attacker.

Proposition 2 *The proposed protocol is robust against MitM attack.*

Proof The aim of this attack is to hijack the communication channel between the UE and the TgNB such that these two entities are unable to determine that they are not directly connected to one another. Suppose that an attacker intercepts {C, A_2, $Ï$, B_1, $\Im_1$, $Ґ_1$} and replaces it with {C^A, A_2, $Ï^A$, $B_1{}^A$, $\Im_1{}^A$, $Ґ_1{}^A$}. However, the composed message is unhelpful to the attacker since B_1 is a keyed message authentication code that is derived over A_1. Here, an attacker is unable to derive valid $A_1 = h(UE_{ID}||T_{ID}||Ï||Ÿ||Ґ_1)$ due to the incorporation of $Ÿ = R_1.\zeta$ that requires UE's secret key ζ. Since ζ is unavailable to the attacker, this attack fails. In addition, an adversary is unable to alter $A_2 = E_{\mathfrak{H}}(UE_{ID}, T_{ID}, Ґ_1)$ without a valid UE secret token $\mathfrak{H}$. Suppose that an attacker has intercepted {D_1, C_1, A_3, B_2, $\Im_2$, $Ґ_2$} and replaces it with {$D_1{}^A$, $C_1{}^A$, A_3, $B_2{}^A$, $\Im_2A$, $Ґ_2{}^A$}. Since the attacker cannot derive valid $B_2 = MAC_{A_1^*}((T_{ID}, Ґ_2, C_1)$ and $A_3 = E_{\mathfrak{H}}(UE_{ID}, T_{ID}, Ґ_2)$, this attack flops.

Proposition 3 *Impersonation attack is not feasible against the proposed protocol.*

Proof Suppose that an attacker wants to masquerade as a legitimate UE. To accomplish this, an adversary randomly selects $R_1{}^A$ and derives $Ï^A = R_1{}^A.Q$ that is deployed to compute bogus message $Ÿ^A$. Afterward, messages $A_1{}^A = h(UE_{ID}{}^A||T_{ID}||Ï^A||Ÿ^A||Ґ_1{}^A)$, $B_1{}^A = MAC_{A_1^A}(UE_{ID}{}^A, Ґ_1{}^A, Ï^A)$ are derived and {$\mathbb{Z}^A$,

$A_{2,}$ $\ddot{I}^A$, $B_1{}^A$, $\Im_1{}^A$, $Ґ_1{}^A\}$ constructed before being transmitted to the TgNB. Since the UE's real identity UE_{ID} is encrypted in $A_2 = E_{\mathfrak{H}}(UE_{ID}, T_{ID,}\ Ґ_1)$, an adversary cannot obtain it and hence fake identity $UE_{ID}{}^A$ will fail the $UE_{ID}{}^* = UE_{ID}$ check. In addition, TgNB cannot establish the correct $A_1{}^A = h(UE_{ID}{}^A||T_{ID}||\ddot{I}^A||\ddot{Y}^A||Ґ_1{}^A)$ due to deployment of fake $\ddot{Y}^A$ instead of $\ddot{Y}^* = \ddot{I}(\mathbb{H} + \mathcal{B}^*)^{-1}$. As such, $B_1{}^* \neq B_1{}^A$ is easily detected at the TgNB. Similarly, an attacker cannot impersonate the TgNB due to lack of TgNB's secret key $\mathbb{H}$, UE's secret token $\mathfrak{H}$ and tracking area identity T_{ID}. Consequently, both UE and TgNB impersonation attacks fail.

Proposition 4 *Forward and backward key secrecy is upheld in the proposed protocol.*

Proof The goal of this security feature is to prevent disclosure of previous as well as future keys upon successful compromise of private keys, session keys, long-term keys or secret keys. Suppose that long-term secret keys $\mathfrak{H}$, ζ and $\mathbb{H}$ of both the UE and TgNB are exposed to the attacker. However, previous session keys cannot be derived since each session key is dynamically and independently computed at the UE and TgNB: $\phi_U = h(UE_{ID}||T_{ID}||\ddot{I}||C_1||D_2)$. Here, $\ddot{I} = R_1.Q$, $C_1 = R_2.Q$, and $D_2 = R_1.C_1$, in which R_1 and R_2 are UE and TgNB random numbers, respectively. According to ECDLP, it is computationally infeasible for an attacker to obtain the real value of these random numbers and hence this attack fails.

Proposition 5 *The proposed protocol is resilient against physical capture attacks.*

Proof Suppose that an attacker physically captures the UE and attempts to learn its secrets so as to launch impersonation attacks against other UEs. However, in the proposed protocol, the secret keys are independently computed at each UE and hence the leaned secrets in one UE cannot compromise the security of other UEs. In addition, each UE has a shared token $\mathfrak{H}$ with the TgNB which is unique for every UE. As such, this attack is not possible in the proposed protocol.

Proposition 6 *Known session key attack is infeasible in the proposed protocol.*

Proof The goal of this attack is to capture messages $\{\mathbb{Z}, A_{2,}\ \ddot{I}, B_1, \Im_1, Ґ_1\}$ and $\{D_1, C_1, A_3, B_2, \Im_2, Ґ_2\}$ after which an attempt is made to compute the session key used in the previous authentication and key agreement phase. However, the proposed protocol establishes shared session keys $\phi_T = h(UE_{ID}||T_{ID}||\ddot{I}||C_1||C_2)$ and $\phi_U = h(UE_{ID}||T_{ID}||\ddot{I}||C_1||D_2)$ whose strength depends on the strength of one-way hash function and the constituent secrets. Since it is computationally infeasible to reverse a one-way hash function, and correctly guess the random numbers, this attack fails against the proposed protocol.

Proposition 7 *The proposed protocol is resilient against DoS.*

Proof There are numerous techniques of launching DoS in cellular networks. For instance, old messages can be replayed toward both the UE and TgNB. To curb this attack, timestamps $Ґ_1$, $Ґ_2$ and $Ґ_3$, and random numbers R_1 and R_2 are incorporated in all the exchanged messages.

Proposition 8 *The communicating entities execute strong mutual authentication and key agreement.*

Proof In the proposed protocol, TgNB authenticates the UE by checking whether $UE_{ID}{}^{*} = UE_{ID}$ while the UE authenticates the TgNB through checking whether $T_{ID}{}^{*} = T_{ID}$. As such, after mutual authentication, the UE and TgNB can establish some trust levels between them. Afterward, session keys $\phi_T = h(UE_{ID}||T_{ID}||\ddot{I}||C_1||C_2)$ and $\phi_U = h(UE_{ID}||T_{ID}||\ddot{I}||C_1||D_2)$ are derived at the TgNB and UE respectively to secure the exchanged packets.

Proposition 9 *Eavesdropping is effectively prevented in the proposed protocol.*

Proof To curb this attack, symmetric cryptosystems are deployed, which include $A_2 = E_{\mathfrak{H}}(UE_{ID}, T_{ID,}\ Ґ_1)$, $B_1 = MAC_{A_1}(UE_{ID}, Ґ_1, \ddot{I})$, $A_3 = E_{\mathfrak{H}}(UE_{ID}, T_{ID,}\ Ґ_2)$ and $B_2 = MAC_{A_1^*}((T_{ID}, Ґ_2, C_1)$. In addition, each UE has unique secret token $\mathfrak{H}$ whose identity is $\mathfrak{R}$. In the proposed protocol, $\mathfrak{H}$ is deployed to encipher $\{UE_{ID}, T_{ID,}\ Ґ_1\}$. On the other hand, TgNB requires corresponding key of $\mathfrak{R}$ so as to decrypt A_2. Moreover, traffic is protected using the computed session keys $\phi_T = h(UE_{ID}||T_{ID}||\ddot{I}||C_1||C_2)$ and $\phi_U = h(UE_{ID}||T_{ID}||\ddot{I}||C_1||D_2)$ so as to curb any packet sniffing.

Proposition 10 *The proposed protocol is robust against bogus message injection attacks.*

Proof Suppose that an attacker attempts to alter the exchanged messages between the UE and TgNB. In the proposed protocol, the UE computes $B_1 = MAC_{A_1}(UE_{ID}, Ґ_1, \ddot{I})$ which is derived over $A_1 = h(UE_{ID}||T_{ID}||\ddot{I}||\ddot{Y}||Ґ_1)$. The incorporation of UE_{ID}, $\ddot{I} = R_1.Q$ and $\ddot{Y} = R_1.\zeta$ and timestamp $Ґ_1$ implies that A_1 can only be derived by a legitimate UE. As such, an attacker is unable to change the exchanged messages through injection of bogus packets.

Proposition 11 *Anonymity of communicating entities is upheld in the proposed protocol.*

Proof Suppose that an attacker eavesdrops the communication channel between the UE and TgNB and spoofs UE_{ID} and $\mathfrak{R}$. However, in the proposed protocol, whenever the UE establishes communication session with TgNB, it does not transmit UE_{ID} in plaintext but enciphers it in $A_2 = E_{\mathfrak{H}}(UE_{ID}, T_{ID,}\ Ґ_1)$. In addition, pseudonymity of $\mathfrak{R}$ is attained through $\mathbb{Z} = h(T_{ID}||\mathfrak{I}_1) \oplus (\mathfrak{R}||Ґ_1)$ and $D_1 = h(T_{ID}||\mathfrak{I}_2||) \oplus (\mathfrak{R}||Ґ_2)$. Consequently, on valid TgNB can derive UE_{ID} through the decryption of A_2 using $\mathfrak{H}$: $D_{\mathfrak{H}}(A_2)$ to yield $UE_{ID}{}^{*}$, $T_{ID}{}^{*}$ and $Ґ_1{}^{*}$. As such, the proposed protocol attains anonymity and is resilient against spoofing attacks.

4.2 Performance Evaluation

In this section, the proposed protocol is evaluated using execution time and bandwidth requirements as key metrics.

Execution time: The cryptographic operations executed in the proposed protocol included MAC operation T_{MAC}, Advanced Encryption Standard (AES) encryption and decryption T_{AES}, point multiplication T_{PM} and hashing operations T_H. Based on the values in [3] and [35], T_{MAC}, T_{AES},T_{PM} and T_H take 39 ms, 20 ms, 1.082 ms and 5 ms, respectively. Table 2 gives the computations involved at the UE and TgNB.

On the other hand, the scheme in [17, 22, 29] and [16] take 1230 ms, 1570 ms, 1020 ms and 780 ms respectively, as shown in Table 3.

Figure 3 shows the graph of execution time for the five authentication protocols. As shown in Fig. 3, the scheme presented in [22] had the highest execution time followed by the schemes in [17, 29] and [16] in that order.

As such, the proposed protocol had the least execution time. Since execution time is directly proportional to the energy consumptions of the supported B5G IoT devices, the proposed protocol is the most ideal for deployment in these IoT devices.

Table 2 Execution time computation

UE	TgNB	Total (ms)
$3T_{PM} + 4T_H + 2T_{MAC} + 2T_{AES}$ $= (3.246 + 20 + 78 + 40)$ $= 141.246$	$3T_{PM} + 5T_H + 2T_{MAC} + 2T_{AES}$ $= (3.246 + 25 + 78 + 40)$ $= 146.246$	$6T_{PM} + 9T_H + 4T_{MAC} + 4T_{AES}$ $= (6.492 + 45 + 156 + 80)$ ≈ 288

Table 3 Execution time comparisons

Protocol	Execution time (ms)
[16]	780
[17]	1230
[22]	1570
[29]	1020
Proposed	288

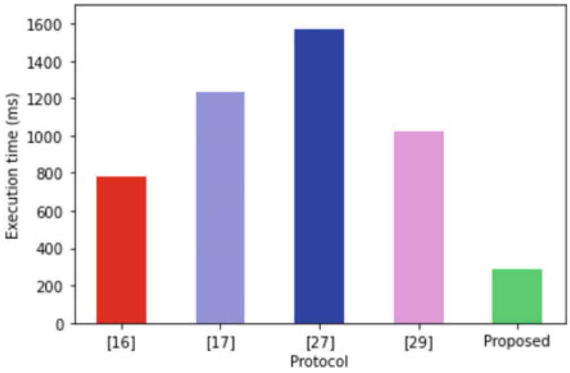


Fig. 3 Execution time comparisons

Bandwidth requirements**:** In this analysis, the values in [3] and [35] are deployed in which symmetric key size, timestamps, identities, pseudo-random numbers, hashing, random numbers and MAC are 16 bytes, 5 bytes, 2 bytes, 32 bytes, 8 bytes, 16 bytes and 8 bytes, respectively, as shown in Table 4.

Using these values, the exchanged messages $A_{Req} = \{\mathbb{Z}, A_{2,} \ddot{I}, B_1, \Im_1, \acute{\Gamma}_1\}$ and $A_{Res} = \{D_1, C_1, A_3, B_2, \Im_2, \acute{\Gamma}_2\}$ are 85 bytes each as shown in Table 5 that follows.

On the other hand, the communication overheads for the scheme in [17, 22, 29] and [16] are 976 bytes, 496 bytes, 490 bytes and 576 bytes, respectively, as shown in Table 6.

Figure 4 shows the graph of the bandwidth requirements for these five authentication protocols. Based on Fig. 4, the protocol in [17] had the highest bandwidth requirements followed by the schemes in [16, 22] and [29] in that order.

As such, the proposed protocol had the least communication overheads among all these schemes. Since bandwidth is a scarce resource, the proposed protocol made

Table 4 Parameter length

Parameters	Size (bytes)
Symmetric key size	16
Timestamps	5
Identities	2
Pseudo-random numbers	32
Hashing	8
Random numbers	16
MAC	8

Table 5 Bandwidth requirement computation

UE	TgNB	Total (bytes)
$\{\mathbb{Z}, A_{2,} \ddot{I}, B_1, \Im_1, \acute{\Gamma}_1\}$ $\mathbb{Z} = B_1 = 8, A_2 = 16, \ddot{I} = 16, \Im_1 = 32,$ $\acute{\Gamma}_1 = 5$ $= (8 + 8 + 16 + 16 + 32 + 5)$ $= 85$	$\{D_1, C_1, A_3, B_2, \Im_2, \acute{\Gamma}_2\}$ $= (D_1 = B_2 = 8, C_1 = A3 = 16, \Im_2 =$ $32, \acute{\Gamma}_2 = 5$ $= (8 + 8 + 16 + 16 + 32 + 5)$ $= 85$	170

Table 6 Bandwidth requirement comparisons

Protocol	Bandwidth (bytes)
[16]	576
[17]	976
[22]	496
[29]	490
Proposed	170

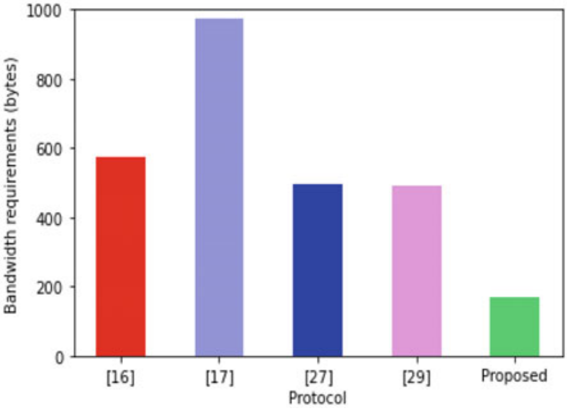


Fig. 4 Bandwidth requirement comparisons

the most efficient utilization of the network bandwidth. Consequently, it is the most ideal for deployment in ultra-dense B5G networks.

5 Conclusion and Future Work

Numerous protocols have been presented in literature to protect the massive data exchanged over the B5G networks. These schemes are based on techniques such as biometrics, elliptic curve cryptography, blockchains and symmetric cryptography. However, these protocols still have high storage, communication costs, execution time, communication latencies and energy requirements. Consequently, they are not ideal for most B5G applications scenarios such as WSN and IoT in which the sensors and actuators have limited energy and computation power. In addition, it has been shown that they are still susceptible to a number of attacks that can be utilized to bring the entire network down. The developed protocol has addressed some of these security and performance issues. In particular, it has been shown to offer anonymity, mutual authentication and both forward and backward key secrecy. In addition, it is robust against attacks such as bogus message injection, eavesdropping, DoS, known session key, physical capture, impersonation, MitM and packet replays. Its ability to exhibit the lowest execution time at the lowest bandwidth requirements makes it applicable in B5G networks. Future work lies in the formal verification of the security features of the proposed protocol. There is also need to evaluate this protocol using metrics that were not within the scope of this work.

Acknowledgements This work is supported by Natural Science Foundation of Top Talent of SZTU (Grant number: 20211061010016).

References

1. Choudhary G, Kim J, Sharma V (2018) Security of 5G-mobile backhaul networks: a survey. J Wirel Mob Netw, Ubiquitous Comput, Dependable Appl 9(4):41–70
2. Nyangaresi VO, Rodrigues AJ, Abeka SO (2020) Neuro-fuzzy based handover authentication protocol for ultra dense 5G networks. In: 2020 2nd Global power, energy and communication conference (GPECOM), IEEE, Izmir, Turkey, pp 339–344
3. Haddad Z, Fouda MM, Mahmoud M, Abdallah M (2020) Blockchain-based authentication for 5G networks. In: 2020 IEEE international conference on informatics, IoT, and enabling technologies (ICIoT), IEEE, pp 189–194
4. Li G, Lai C (2020) Platoon handover authentication in 5G-V2X: IEEE CNS 20 poster. In: 2020 IEEE conference on communications and network security (CNS), IEEE, 1–2
5. Wu TY, Lee Z, Obaidat MS, Kumari S, Kumar S, Chen CM (2020) An authenticated key exchange protocol for multi-server architecture in 5G networks. IEEE Access 8:28096–28108
6. Nyangaresi VO, Rodrigues AJ, Abeka SO (2020) Efficient group authentication protocol for secure 5G enabled vehicular communications. In: 2020 16th International computer engineering conference (ICENCO), 25–30, IEEE, Cairo, Egypt
7. Zhang Z, Zhang W, Qin Z, Hu S, Qian Z, Chen X (2021) A secure channel established by the PF-CL-AKA protocol with two-way ID-based authentication in advance for the 5G-based wireless mobile network. In: 2021 IEEE Asia conference on information engineering (ACIE), IEEE, 11–15
8. Shin S, Kwon T (2020) A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things. IEEE access 8:67555–67571
9. Nyangaresi VO (2021) Lightweight key agreement and authentication protocol for smart homes. In: 2021 IEEE AFRICON, IEEE, 1–6
10. Ouaissa M, Houmer M, Ouaissa M (2020) An enhanced authentication protocol based group for vehicular communications over 5G networks. In: 2020 3rd International conference on advanced communication technologies and networking (CommNet), IEEE, 1–8
11. Nyangaresi VO, Rodrigues AJ, Abeka SO (2021) ANN-FL secure handover protocol for 5G and beyond networks. In: Zitouni R, Phokeer A, Chavula J, Elmokashfi A, Gueye A, Benamar N (eds) Towards new e-Infrastructure and e-Services for developing countries. AFRICOMM 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 361. Springer, Cham
12. Fang D, Qian Y (2020) 5G wireless security and privacy: Architecture and flexible mechanisms. IEEE Veh Technol Mag 15(2):58–64
13. Fang H, Wang X, Tomasin S (2019) Machine learning for intelligent authentication in 5G and beyond wireless networks. IEEE Wirel Commun 26(5):55–61
14. Benzaid C, Taleb T (2020) AI for beyond 5G networks: a cyber-security defense or offense enabler? IEEE Network 34(6):140–147
15. Nyangaresi VO (2021) ECC based authentication scheme for smart homes. In: 2021 International symposium ELMAR, IEEE, 5–10
16. Braeken A, Liyanage M, Kumar P, Murphy J (2019) Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks. IEEE Access 7:64040–64052
17. Koutsos A (2019) The 5G-AKA authentication protocol privacy. In: 2019 IEEE European symposium on security and privacy (EuroS&P), pp 464–479
18. Refaey A, Hammad K, Magierowski S, Hossain E (2020) A blockchain policy and charging control framework for roaming in cellular networks. IEEE Network 34(3):170–177
19. Rivera AV, Refaey A, Hossain E A blockchain framework for secure task sharing in multi-access edge computing. IEEE Netw 35(3):176–183
20. Nyangaresi VO, Petrovic N (2021) Efficient PUF based authentication protocol for Internet of drones. In: 2021 International telecommunications conference (ITC-Egypt), IEEE, 1–4

21. Chen M, Tan C, Zhu X, Zhang X (2020) A blockchain-based authentication and service provision scheme for Intemet of Things. In: 2020 IEEE globecom workshops (GC Wkshps), IEEE, 1–6
22. Gharsallah I, Smaoui S, Zarai, F (2019) A secure efficient and lightweight authentication protocol for 5G cellular networks: Sel-aka. In: 2019 15th international wireless communications mobile computing conference (IWCMC), pp 1311–1316
23. Haddad Z, Mahmoud M, Taha S, Saroit IA (2015) Secure and privacy-preserving ami-utility communications via lte-a networks. In: 2015 IEEE 11th international conference on wireless and mobile computing, networking and communications (WiMob), IEEE, pp 748–755
24. Zhou J (2015) A quadratic residue-based lightweight RFID mutual authentication protocol with constant-time identification. Journal of Communications 10(2):117–123
25. Nyangaresi VO, Mohammad Z (2021) Privacy preservation protocol for smart grid networks. In: 2021 International telecommunications conference (ITC-Egypt), IEEE, 1–4
26. Hsu R, Lee J, Quek TQS, Chen J (2018) Graad: Group anonymous and accountable D2D communication in mobile networks. IEEE Trans Inf Forensics Secur 13(2):449–464
27. Wang M, Yan Z (2018) Privacy-preserving authentication and key agreement protocols for d2d group communications. IEEE Trans Industr Inf 14(8):3637–3647
28. Nyangaresi VO, Rodrigues AJ, Taha NK (2021) Mutual authentication protocol for secure VANET data exchanges. In: International conference on future access enablers of Ubiquitous and intelligent infrastructures, Springer, Cham, pp 58–76
29. Liu F, Peng J, Zuo M (2018) Toward a secure access to 5G network. In: 2018 17th IEEE international conference on trust, security and privacy In computing and communications/ 12th IEEE international conference On Big Data science and engineering (TrustCom/BigDataSE), IEEE, pp 1121–1128
30. Wong AMK, Hsu CL, Le TV, Hsieh MC, Lin TW (2020) Three factor fast authentication scheme with time bound and user anonymity for multi-server E-health systems in 5G-based wireless sensor networks. Sensors 20(9):2511
31. Le TV, Hsu CL (2021) An Anonymous Key Distribution Scheme for Group Healthcare Services in 5G-Enabled Multi-Server Environments. IEEE Access 9:53408–53422
32. Wu F, Li X, Xu L, Sangaiah AK, Rodrigues JJ (2018) Authentication protocol for distributed cloud computing: An explanation of the security situations for Internet-of-Things-enabled devices. IEEE Consumer Electronics Magazine 7(6):38–44
33. Sahay R, Blanc G, Zhang Z, Debar H (2017) ArOMA: An SDN based autonomic DDoS mitigation framework. Comput Secur 70:482–499
34. Bawany NZ, Shamsi JA(2019) SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks. J Netw Comput Appl 145:102381
35. Xue K, Meng W, Zhou H, Wei DS, Guizani M (2020) A lightweight and secure group key based handover authentication protocol for the software-defined space information network. IEEE Trans Wireless Commun 19(6):3673–3684

Measuring the Uptaking of Digital Health Platforms on AAL/AHA Domain

Carlos Juiz, Belen Bermejo, Alexander Nikolov, Silvia Rus, Andrea Carboni, Dario Russo, Davide Moroni, Efstathios Karanastasis, Vassiliki Andronikou, Christina Samuelsson, Frederic Lievens, Ad van Berlo, Willeke van Staalduinen, and Maria Fernanda Cabrera-Umpierrez

Abstract This paper presents a method to determine the metrics to assess the uptake of Ambient Assisted Living (AAL) platforms. The different platforms are offering various resources to construct digital health products oriented to Active and Healthy Aging (AHA) and social health care. This research work is addressed to identify and define which metrics could be Key Performance Indicators (KPIs) to be tracked for successful uptake, interoperability, synergies, and cost–benefit analysis of open platforms.

Keywords Uptaking · Digital health platforms · AAL · AHA KPIs

C. Juiz (✉) · B. Bermejo
Computer Science Department, University of the Balearic Islands, Palma, Spain
e-mail: cjuiz@uib.es

A. Nikolov
SYNYO GmbH, Vienna, Austria

S. Rus
Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany

A. Carboni · D. Russo · D. Moroni
National Research Council, Institute of Information Science and Technologies, Pisa, Italy

E. Karanastasis · V. Andronikou
School of Electrical and Computer Engineering, National Technical University, Athens, Greece

C. Samuelsson
Department of Biomedical and Clinical Sciences, Linköping University, Linköping, Sweden

F. Lievens
Lievens-Lanckman Bvba, Grimbergen, Belgium

A. van Berlo
Smart Homes, Maarssen, Netherlands

W. van Staalduinen
AFEdemy, Academy On Age-Friendly Environments in Europe BV, Gouda, Netherlands

M. F. Cabrera-Umpierrez
Universidad Politécnica de Madrid, Madrid, Spain

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_45

1 Introduction

Aging presents one of the greatest socio-economic challenges in the twenty-first century. Our research project aims at analyzing open service platforms in the AHA and AAL fields and the measurement of their performance. To do this, a set of KPIs needs to be defined to perform effective analysis of the platforms' success. As the platforms' success involves more than one factor for more than one stakeholder group to make it measurable in detail, a set of KPIs is defined and analyzed according to a specific methodology.

Key European domain-related platforms are relevant, such as universAAL IoT [1] and FIWARE [2]. Besides the two mentioned platforms, a considerable number of platforms have been created and are operational on similar services within the similar domain, either competing or complementing each other, which would urge for more interoperability among them. Responding to the numerous critical voices, lack of interoperability of the various solutions deployed, or difficulties with the large-scale uptake of the platforms by their targeted users, the main objective of this research is to determine the platforms' uptake by their user communities as well as their continuous improvement and possibility of market expansion. Consequently, the research question of this work attempt to answer is how this platform uptake can be measured and quantified? The response to this question should serve to measure the uptake in current and future AAL platforms.

2 State of the Art

We collect the existing open-source platforms that belong to the bigger ecosystem together with universAAL IoT, FIWARE, and include those that are partly open or fully proprietary. The selection concerned three types of projects; those aimed specifically at AAL/AHA issues, projects for general purposes but application guaranteed by the AAL/AHA environment, and projects that brought specific integrated development and innovation in the sector. These projects are: ACTIVAGE/AIOTES, VAALID, UNCAP, ReAAL, BEYOND SILOS, universAAL, PERSONA, GIRAFF+, eWALL, FI-STAR, m-power, HAH, ACCOMPANY, HDIM, FIWARE, AmIVital, CareWell, ehcoBUTLER, INNOVAGE, SOPRANO, AMIGO, Mario, Reach2020, SmartCare, CARER + and EkoSmart. In this research work, we focus on universAAL IoT and FIWARE as reference platforms due to their popularity.

3 Problem Statement

A Key Performance Indicator (KPI) is a measurable value that represents the possibility of a process or action of a company or organization, to achieve a specific

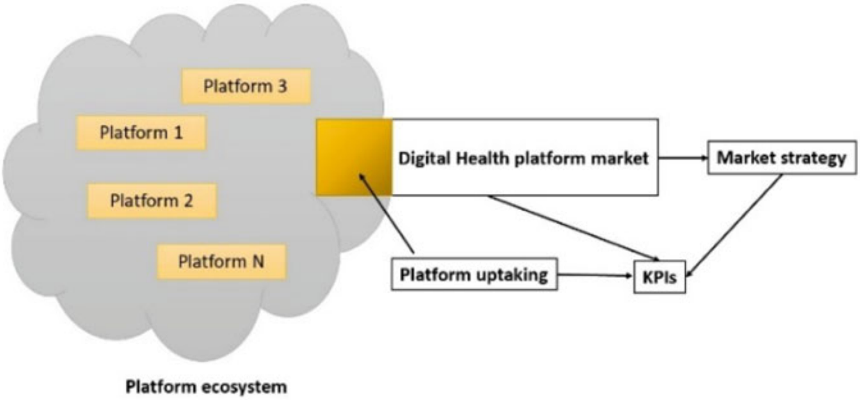


Fig. 1 Overview of problem statement

objective (mainly strategic). While a metric measures a raw value on a process, a KPI is directly associated with a goal set by the organization and allows to assess whether the strategies followed to achieve it are working. Since this work aims to analyze the uptake of the existing platforms in the AHA/AAL field, a set of KPIs needs to be defined to perform an effective analysis of the platforms' success.

Thus, it seems that the number of users of these platforms may partially define the platform uptake. However, considering the market strategy and the use of the platforms, a set of KPIs can be defined to determine the platforms' uptake (see Fig. 1).

4 Methodology for the Definition of Potential KPIs

In our research, we propose different stakeholders types around any platform, such as: primary end-users (the single individual intended as the main beneficiary of a service or set of services provided by the considered platform), end-user customer (the person or organization in direct contact with a primary end-user, such as formal and informal care persons, family members, care organizations, and their representatives), technology providers (typically hired by customer end-users that follow and implement the entire life cycle of the applications), and government (the public sector service organizers, social security systems, insurance companies). In this work, we propose a methodology to determine the platforms' uptake. This methodology is divided into four steps, and it aims to obtain a list of representative KPIs for platform uptake:

1. The first step regards the ecosystem observation by reviewing whether some platform is publicly showing a set of metrics and/or even KPIs of its uptake. This direct information should be crawled in the sites of the different platforms.

This first step also includes indirect information coming from research papers related to this uptake. Thus, a literature review is necessary. In any case, if positive, recapture all these metrics or KPIs from reviews and jump to step 3.

2. In case of not having metrics or KPIs from step 1, proceed with different benchmarking procedures with other platform sectors as the software platforms or e-commerce platforms to determine potential metrics or KPIs. Any potential metric or KPIs should be translated to the AHA/AAL domain. Additionally, the authors as researchers in the domain add other potential metrics or KPIs not provided by benchmarking.
3. Make a proposal of KPIs (classified by stakeholder types and pointing out which are generic vs. AHA/AAL specialized).
4. Propose the potential list of KPIs and metrics to stakeholders through different instruments. Then, considering the platform's stakeholders' experience and intention, the list of uptake KPIs shall be obtained as a result of the application of the proposed methodology.

4.1 Platform Review and Literature Review

After the review of the complete list of platforms above, we did not find any metric or KPI to assist with the platform uptake assessment. Thus, we proceeded with a partial systematic literature review. To determine the platforms' uptake, a revision of outcomes from the literature was performed for the two more popular platforms (one generic and one specialized), aiming to get information on potential KPIs that will nurture our analysis. Some keywords were identified to perform a Google Scholar search (i.e., "KPI", "Key performance indicator", "metric", "measure", "benchmarking", "AHA", "AAL" and "platform"). Then, these logical expressions (LE) were used for the search:

- LE1: "FIWARE" AND (("KPI" OR "Key performance indicator" OR "metric" OR "measure" OR "benchmarking") AND ("AHA" OR "AAL" OR "platform"))
- LE2: "UNIVERSAAL" AND (("KPI" OR "Key performance indicator" OR "metric" OR "measure" OR "benchmarking") AND ("AHA" OR "AAL" OR "platform")).

Taking into account the whole metadata from Google Scholar and with any timeline restrictions, we obtained 983 results from LE1 and 293 from LE2. In a second stage, we obtained from the abstract information that the platform's performance is the main aim of the current literature. Therefore, we modified the LE1 and LE2 to go in-depth on the performance study, evaluating the modified logical expressions in the same previous conditions:

- LE1.1: "FIWARE" AND (("KPI" OR "Key performance indicator" OR "metric" OR "measure" OR "benchmarking") AND ("AHA" OR "AAL" OR "platform") AND "performance")

- LE2.1: “universAAL” AND ((“KPI” OR “Key performance indicator” OR “metric” OR “measure” OR “benchmarking”) AND (“AHA” OR “AAL” OR “platform”) AND “performance”).

From LE1.1, we obtained 833 results and 205 from LE2.1. From this literature review and our knowledge, there is no paper about metrics of uptaking in AHA/AAL domains. Then we proceeded with reviewing the whole list of platforms. However, we were not able to establish any consequent and consistent list of metrics or KPIs for any platform publishing its uptake measurements as there is no research paper about this. To solve this problem, we proceed with step two of our methodology.

4.2 Benchmarking

As we denoted in the previous section, it is necessary to proceed with the benchmarking process to obtain a potential list of metrics and KPIs for uptake. We followed the benchmarking methodology proposed by Kaiser Associates [3]. The obtained list of metrics and KPI is not specialized in AAL/AHA domain, and we should adapt it to our domain.

5 Proposal of Metrics and KPIs (Results)

In the following, we present a set of KPIs from different stakeholders’ perspectives to determine the degree of platform uptake. There are 12 KPIs that can be specialized for the digital health domain marked with (S).

5.1 KPIs for Primary End-Users

- Reaching user goals, needs, and preferences: The platform matches the user’s goals, needs, and preferences, which may be specific to the context of use and are subject to change.
- Accessibility: The platform is accessible for persons with disabilities, and older persons is a prerequisite for personal user experience.
- User-driven design: The platform has been developed with user involvement.
- User empowerment: The platform significantly contributes to the individual user’s empowerment, by supporting and training the individual user to better understand and express their current and future wishes, needs, and preferences.
- Adaptability: The user should be able to adjust the look & feel of the platform and overwrite the system’s choices and interface settings.

- Non-stigmatization: The platform looks attractive and is meaningful to everyone. It does not exclude any subgroup of users.
- Easy to use: The platform is easy to use.
- Responsive: The platform adapts itself to the user's selected preferences, behavior, and devices.
- Modular: It allows the user to extend the solution by adding additional modules, if needed.
- Privacy and data governance: The platform provides information on data collection, access, usage, control, sharing, and benefit to the user.
- Ethics compliance: The platform ensures that complies with de facto ethical issues such as the Declaration of Helsinki.
- Autonomy: The level of autonomy of users reached using the platform.
- Hospitalizations (S): The percentage of hospitalizations of end-users using the platform compared with current clinical practices without the usage of the platform.
- Quality of Life: Quality of Life: impact on QoL of the platform services.
- Learnability: The platform and its functions are learnable for both older persons, relatives, and staff.
- Interest and enjoyment: The platform is interesting and enjoyable to end-users; older adults, relatives, and staff.
- Costs for informal care (S): The costs decrease/increase of informal care for end-user using the platform.
- K-factor for attracting other end-users: used to describe the growth rate of platform users, the platform-developed apps, or membership of the platform.
- Adherence-health + app/solution (S): The end-users are improving due to the app/solution developed based on platform contents.
- Affordability-treatment + app/solution (S): Treatment became more affordable end-users because of the developed app/solution based on platform contents.
- Efficiency-treatment + app/solution (S): Treatment is more efficient because the developed app/solution based on platform contents was used/solution.
- Effectiveness-treatment + app/solution (S): Treatment process is more effective because the developed app/solution based on platform contents was used (except for clinical effectiveness).
- Empowerment-app/solution (S): The app/solution developed based on platform contents empowers the end-users and health professionals to know more about their conditions or perform their tasks better.
- Safety-app/solution: The developed app/solution based on platform contents itself is safe or makes the treatment process safer.
- Trustability-treatment + app/solution (S): The developed app/solution based on platform contents improves the trust of the end-user in the treatment.
- Customer Success Stories Submitted: The amount of Customer Success Stories Submitted.

5.2 KPIs for End-User Customers

- Compliance/Adherence to standards: These would make the platform directly compatible with hardware (e.g., medical or other IoT devices), software (e.g., services or tools), or another kind of protocols (e.g., compliance to legal/ethics/security requirements via standards).
- The wideness of adoption of the platform: Number of users of the platform.
- Availability/Level of support: Number of available support channels.
- Maintenance difficulty level: How easy or difficult is it to locate and fix problems with the platform.
- Mean frequency of updates: How often are existing problems tackled.
- Monitoring capabilities (or other capabilities of high importance for IoT): Performance issues can be quickly understood and resolved.
- Compliance/Adherence to standards: These would make the platform directly compatible with hardware (e.g., medical or other IoT devices), software (e.g., services or tools), or another kind of protocols (e.g. compliance to legal/ethics/security requirements via standards).
- Minimal fixed cost: Initial cost for purchasing the required platform components.
- Readability of platform documentation: How much time did it take to go through all platform documentation.
- Platform deployment: How much time did it take to deploy the platform.
- Platform configuration: How much time did it take to configure the different tools/components of the platform.
- Platform support documentation: How good are the platform installation and configuration documentation.
- Platform support services: How good are the provided support services (e.g., phone/email/chat support) for the platform.
- Awareness (TOMA) (S): Top of mind: The first platform that comes to mind when a stakeholder is asked an unprompted question about AHA/AAL.
- Acquisition (registration/membership…): registration on the platform.
- Revenue (gross receipts, support, contributions, etc., gains, gross income…): Economic revenue of platform.
- Average producer/developer/… lifespan: It is the average number of years that a service producer/developer continues to produce through the platform's components/items/…
- Retention (active producers/developers/…): It is the percentage of active producers/developers from total (registered, known).
- K-factor for attracting other producers/developers/registrations/donations/…: the K-factor can be used to describe the growth rate of platform users, the platform-developed apps, or membership of the platform.
- Productivity: The number of solutions based on platform contents over time.
- Robustness: The number of use-cases based on platform contents over time.
- Certifications of apps/solutions: The number of certifications of apps/solutions based on platform contents.

5.3 KPIs for Technology Providers

- Initial investment: The costs related to the setup of the platform (e.g., hardware, software royalties, installation, and configuration).
- Cost per year: The costs to maintain the platform actively.
- Cost per user: The mean costs for each user.
- Reduction of home care costs (S): The decrease of hospitalization of end-user using the platform.

5.4 KPIs for Government

- The efficiency of service providers (S): The service providers (including caregivers) find it easy to use the platform, and make fewer errors.
- One Business Model (BM) per user group: The platform offers a BM for each of the user groups addressed.
- Purchasing and usage expectations: The platform considers all stakeholders, including buyer, payer, user, prescriber, and service provider, and their expectations in the purchase and later also in the usage processes.
- Affordability (S): The platform considers its affordability for each of the user groups (who may not be able to pay for it) and supports them in the application of some financial support.
- Sustainability: The platform uses mainstream technologies as much as possible for economic sustainability and easy replacement and updates.
- Usability and acceptance: The usability and acceptance of the services offered by the platform by stakeholders.
- Integration: The platform permits the integration of different devices and integrate/can be integrated with other systems.
- Scalability: The platform can be adapted according to the number of services/users.
- Solve real needs: The platform solves the real needs of end-users.
- Openness: The platform is openly accessible for everyone.
- Churn rate (contributors/members/registrations/…): It is the proportion of subscribers/members/registered/who leave a platform during a given period.
- Engagement per visit (downloads): the visits to the website platforms and the number of downloads of items on the platform.
- Engagement per visit (time spent): the time visiting the website platforms.
- Net Promoter Score (NPS): Scoring of the platform from any stakeholder.
- Literature rate: The number of papers or projects reporting platform usage.

6 Discussion, Conclusion, and Open Problems

The work started with an analysis of current literature with a focus on two widely used reference platforms (i.e., FIWARE and universAAL), where we did not find any relevant KPI that serves to measure the uptake and success of these platforms. According to the authors' knowledge, there is a clear absence of KPIs that help to assess open service platforms aiming to support its success and uptake. This could mean that there is an apparent lack of strategy for platform uptake. KPIs have been analyzed, clustered, and prioritized according to four different perspectives defined by four groups of stakeholders. However, having a KPI does not mean that the stakeholder of this group must provide the necessary information to calculate such KPI. As shown on the measurement instrument and unit fields, in most of the cases, information to measure the KPIs will be provided by others (e.g., platform owners according to the characteristics of the platform or technical features, service providers, etc.). From this research outcome, we cluster the most important KPIs for the different stakeholders. The list of KPIs was developed with a holistic perspective to be applicable for any platform. Moreover, we will consider other commercial platforms different from European projects.

Acknowledgements This research work was co-funded within the project PlatformUptake.EU from European Union's Horizon 2020 research and innovation program under the grant agreement No. 875452.

References

1. "UNIVERsal Open Platform and Reference Specification for Ambient Assisted Living | UniversAAL Project | FP7 | CORDIS | European Commission." https://cordis.europa.eu/project/id/247950/it, Retrieved March 28 2020
2. "The Open Source Platform for Our Smart Digital Future." FIWARE, https://www.fiware.org/, retrieved March 28 2020
3. Beating the competition: a practical guide to Benchmarking (1988) Kaiser Associates, Washington, DC, p 176. ISBN 978-1-56365-018-5. Archived from the original on 2009-08-27. Retrieved 2009-07-14

Improving Arabic Hate Speech Identification Using Online Machine Learning and Deep Learning Models

Hossam Elzayady, Mohamed S. Mohamed, Khaled Badran, and Gouda Salama

Abstract Due to the rising use of social media platforms on a global scale to interact and express thoughts freely, the spread of hate speech has become very noticeable on these platforms. Governments, organizations, and academic institutions have all spent substantially on discovering effective solutions to handle this issue. Numerous researches have been performed in several languages to find automated methods for identifying hate speech, but there has been minimal work done in Arabic. The findings of a performance evaluation of two machine learning models, namely the passive-aggressive classifier (PAC) and the Bidirectional Gated Recurrent Unit (Bi-GRU) augmented with an attention layer, are investigated in this work. Proposed models are developed and evaluated using a multi-platform Arabic hate speech dataset. We employ term frequency-inverse document frequency (TF-IDF) and Arabic word embeddings for feature extraction techniques after running a variety of pre-processing steps. The experimental results reveal that the two proposed models (PAC, Bi-GRU with attention layer) provide an accuracy of 98.4% and 99.1%, respectively, outperforming existing methods reported in the literature.

Keywords Arabic hate speech · Text mining · Online machine learning · Deep learning

1 Introduction

With growing of Internet use, the number of people using social networks (OSN) has also risen dramatically. OSN is now the most widely used and participative platform for expressing feelings, communicating, and transferring information [1,

H. Elzayady · M. S. Mohamed (✉) · K. Badran · G. Salama
Department of Computer Engineering, Military Technical College, Cairo, Egypt
e-mail: mohamedms@mtc.edu.eg

K. Badran
e-mail: khaledbadran@mtc.edu.eg

G. Salama
e-mail: gisalama@mtc.edu.eg

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_46

2]. As a result of the ease of social media platforms' accessibility and anonymity, this provides a fertile atmosphere for the dissemination of violent and damaging information because of the user's desire to dominate discussion and to share their beliefs or arguments [3]. Identifying hate speech on social media is a challenging task at the moment. Text written with the intention of injury, violence, or societal upheaval directed against a particular group is referred to as hate speech [4].

This form of behavior is both socially and psychologically detrimental to users, shaking their confidence in online social media [5]. Some nations and governments throughout the world have implemented laws to limit hate speech on social media platforms. Furthermore, a large number of organizations and firms are now required to assess hate speech on their platforms and take the necessary action (e.g., deletion) [6]. Hate speech on social media has been the subject of several studies that have developed a wide variety of approaches, concentrating on the English language, while there is a dearth of studies on Arabic language [7]. There are more than a billion people who speak Arabic as a first language, and it is the internet's fifth most popular language [8]. As a result of its morphological complexity and inherent ambiguity, handling Arabic language has proven to be difficult. Additionally, Arabic includes a huge number of dialects [9].

In this paper, our goal is to build two efficient models to detect Arabic hate speech. The first model is based on implemented online supervised learning classifier, namely the passive-aggressive classifier (PAC). PAC is generally used for large-scale learning. It is one of the few 'online learning algorithms'. Online machine learning techniques employ sequential input data, and the model is updated step by step. This method does not rely on pre-existing training data, as in traditional batch learning approaches. The second model is based on developed (BI-GRU), with an attention mechanism added to the network model, providing key words with a larger weight and non-key words with a lower weight, allowing important features to stand out more.

In the rest of this paper, related work is provided in Sect. 2. Section 3 explains the proposed methodology, including the dataset description, text preparation steps, feature extraction methods, and classification models. The experimental outcomes are discussed in Sect. 4. Finally, Sect. 5 illustrates the conclusion and future work.

2 Related Work

Recently, there has been a dearth of research on Arabic natural language processing. The identification of online hate speech in an Arabic context has received little attention [10]. However, Al-Hassan and Al-Dossari [11] provided a research on text mining methodologies for dealing with hate speech in general, as well as issues for dealing with hate speech in the Arabic-speaking world. Husain and Uzuner [6] examined the most advanced natural language processing (NLP) approaches for Arabic offensive language identification, encompassing a wide range of topics such as hate speech, cyberbullying, pornography, and violent content. Haddad et al. [12]

constructed the first Arabic benchmark dataset in the Tunisian dialect known (T-HSAB). The dataset comprises 6,039 comments divided into three categories: hateful, abusive, and normal. Although they indicated that the comments were gathered from several platforms, they made no indication of which ones. In order to assess classification performance, classical machine learning classifiers used unigrams, bigrams, and trigrams were applied. All of the models were outperformed by the Naive Bayes (NB) model. Similarly, Mulki et al. [13] built a Twitter dataset for detecting hate speech and abusive language in the Levantine dialect named (L-HSAB), which seeks to prevent any hazardous words from being used automatically. Albadi et al. [14] introduced the first Arabic Twitter dataset to address the issue of religious hate, but they didn't come across any other kinds of hate speech. The dataset is used to train different classification models utilizing lexicon-based, ngrams-based, and deep-learning-based techniques. In terms of area under curve (AUC), gated recurrent unit (GRU) and pre-trained word embedding models excel over all other implemented models, earning a score of (84%). Elmadany et al. [15] used the publicly available (OSACT) dataset [16], in order to perform an Arabic hate speech detection task. Multiple M-BERT-based classifiers were employed with various fine-tuning settings. Macro F1 scores in this task didn't achieve remarkable progress comparable to those found in previous research that used more standard machine learning approaches. Hassan et al. [17] pre-processed the prior dataset (OSACT), for building a hybrid model of support vector machine (SVM) and deep neural networks for identifying abusive language. On the test set, the proposed model received an F1 score of 90.5%. Omr et al. [5] developed a binary system using 12 machine learning classifiers and two deep learning classifiers, presenting the first multi-platform dataset for Arabic hate speech identification. The RNN model had the greatest F1 score of 98.7%, with same accuracy, recall, and precision.

3 Methodology

The overall architecture of our approach is shown in detail in Fig. 1. Feature extraction techniques are applied to the dataset after it has been pre-processed using text mining techniques. Then PAC and BI-GRU models with an attention layer are applied for training. Finally, performance metrics are utilized for model evaluation.

3.1 Dataset Description

In our study, we have taken into account the first multi-platform dataset to identify hate speech in Arabic, which was gathered by [5]. Four social media networks contributed comments: Twitter, YouTube, Facebook, and Instagram. The dataset is well-balanced, unlike many others in previous work. There are a total of 10,000

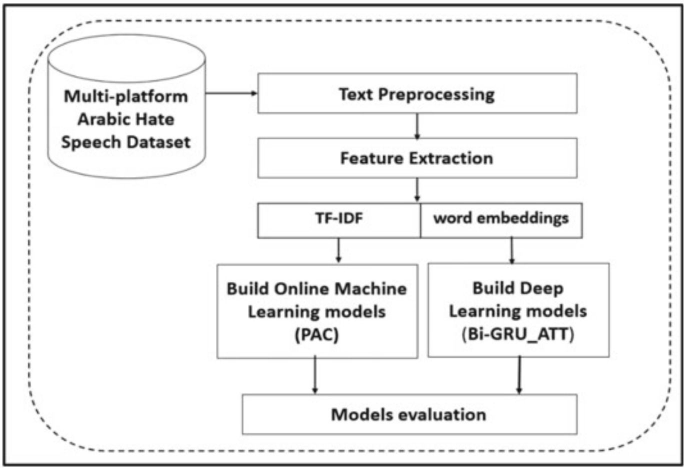

Multi-platform Arabic Hate Speech Dataset
Text Preprocessing
Feature Extraction
TF-IDF
word embeddings
Build Online Machine Learning models (PAC)
Build Deep Learning models (Bi-GRU_ATT)
Models evaluation

Fig. 1 Overview of methodology

Fig. 2 Word cloud of the multi-platform hate speech dataset

hateful comments, but there are also 10,000 non-hateful remarks. Figure 2 shows the world cloud of the utilized dataset.

3.2 Data Pre-processing

This is a vital step in data analysis since it eliminates data that is not strictly essential for the investigation. Pre-processing includes: deleting stop words, neglecting diacritics, discarding hashtags, eliminating punctuation, erasing links, remove empty lines, and normalizing Arabic letters as well as converting emoji and emoticons.

Finally, to guarantee that only Arabic-based letters remain when the process is completed, we utilize the alphabet-detector Python package.

3.3 Feature Extraction

We used term frequency-inverse document (TF-IDF) and word embeddings as our major feature extraction techniques since they are straightforward and problem-independent. First, TF-IDF calculates the relevance of a word to a document in a set of documents [2, 18]. As a result, this technique of operation distinguishes between common and significant words. Second, the most widely used distributed representation of terms is word embeddings. This makes it possible to investigate and identify any word similarity [7]. For Arabic word embedding architectures, we used the pre-trained AraVec2.0 [2].

3.4 Classification Models

Supervised online learning and deep neural networks are used as classification models in our experiments, as stated in the following subsections.

Passive-aggressive classifier. PAC is a notable classifier in online learning algorithms. If the classification produces the desired outcome, this algorithm remains inactive. However, it gets aggressive if the categorization produces an inaccurate result. It does not converge, in contrast to the majority of other algorithms [19]. The key premise of this algorithm is that it observes data, learns from it, and then discards it without retaining it. A classification upgrade is accomplished by solving a restricted optimization problem: The new classification should be as close to the previous one as feasible, with at least a unit margin on the most recent cases [19, 20]. In the face of noise, forcing a unit margin might be excessively aggressive. The passive-aggressive classifier takes a matrix of TF-IDF features as input. As a result, a model is constructed that is trained on the data from the training set and then applied to the test set to assess the classification's performance.

Bidirectional Gated Recurrent Unit with Attention. Two control gates, a reset gate and an update gate, are included in the GRU neural network [21]. Bi-GRU is a sequence processing model made up of two GRUs. One takes information in a forward direction, whereas the other takes it backwards [22, 23]. Text categorization using the Bi-GRU approach relies on associations between words. Instead than using keyword significance in selecting a text's categorization, they evaluate all words equally. By augmenting BI-GRU with an attention mechanism, it is possible to learn which words are more critical to the categorization by giving these keywords a larger weight. Results in a variety of text categorization tasks have been demonstrated to be improved by using this mechanism [23, 24].

4 Experimental Analysis and Results

The results and assessment of the implemented models are presented in this section. All tests are done in Google Colab Pro by using: NumPy, pandas, re, Alphabet Detector, Sklearn, and Keras packages. The results are determined in accordance with the accuracy, precision, recall, and F1 score values.

$$\text{Accuracy} = \frac{\text{Correct Predictions}}{\text{Total Predictions}} \tag{1}$$

$$\text{Precision} = \frac{\text{True positive}}{\text{True positive} + \text{false positive}} \tag{2}$$

$$\text{Recall} = \frac{\text{True positive}}{\text{True positive} + \text{false negative}} \tag{3}$$

$$F1 - \text{score} = 2 \times \frac{(\text{Precision} \times \text{Recall}\ )}{\text{Precision} + \text{Recall}} \tag{4}$$

In order to evaluate our suggested models and compare it with approach proposed in [5], experiments are carried out using a multi-platform Arabic hate speech dataset with a total of 20,000 categorized comments, as described in (3.1). Pre-processing techniques which described in (3.2) are applied for getting rid of any noise from the dataset. Training and test sets are generated from the dataset. The training phase consumes 80% of the data, whereas the testing process consumes 20% of the data (Table 1).

We suggested two models, the first of which is based on PAC algorithms and was trained using the TF-IDF technique. The second model is built on BI-GRU and has an attention mechanism; the model is trained using pre-learned word embeddings (AraVec 2.0). Table 2 displays the parameters used in BI-GRU with attention model.

The results acquired by all the algorithms for the various performance measures are shown in Table 2. According to Table 2, it is obvious that deep learning performs a little better than online machine learning, and BI-GRU with attention is the best

Table 1 Tuned values of the hyperparameters

Hyperparameter	Value
Embedding dimension	300
Loss function	Categorical_crossentropy
Bidirectional GRUs unit	64
Optimizer	Adam
Batch size	128
Dropout	0.5
Number of epochs	10

Table 2 Models' evaluation performances

Model	Accuracy	Precision	Recall	F1_score
PAC (%)	98.4	98.51	98	98.42
BI-GRU with attention (%)	99.1	99.2	99.1	99.1

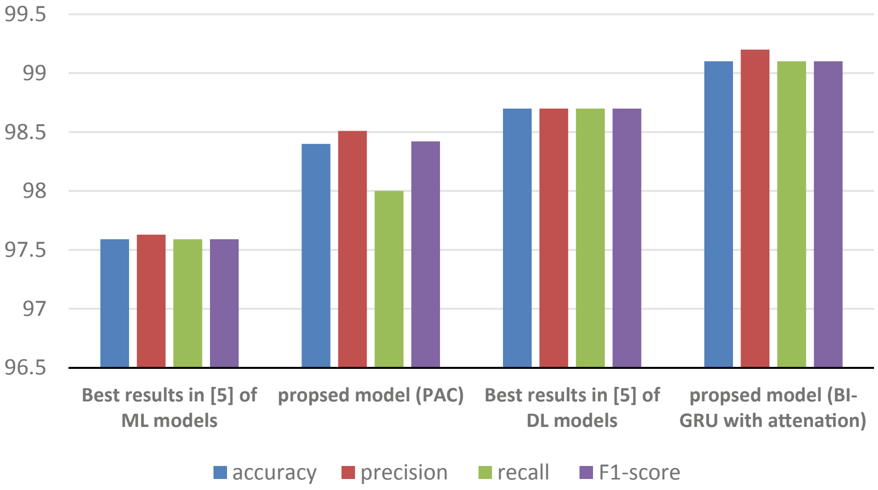


Fig. 3 Performance evaluation of our proposed Arabic hate speech detection models using ML compared with models in [5]

architecture for classifying Arabic hate speech in online social networks with an accuracy of 99.1%, F1 score of 99.1%, recall of 99.1%, and precision equal to 99.2%.

The effectiveness of our proposed methodology in comparison to the comparative methodology in [5] is shown in Fig. 3. In light of the findings, we have discovered some interesting observations. First, the results show that our proposed model BI-GRU with attention is clearly superior to the online machine learning PAC and comparative approach including traditional machine learning and recurrent neural network models. Second, our proposed model based on online machine learning algorithm PAC exhibited the best performance, outperforming all classical machine learning models used in [5]. Finally, it can be deduced that our suggested model Arabic hate speech BI-GRU with attention performed the best when compared to the other described in the related work section.

5 Conclusions

In this study, we identify hate speech in Arabic social media using the first Arabic hate speech dataset gathered from several platforms. We suggest two effective models using the online machine learning algorithms PAC and Bi-GRU augmented by an attention layer. Several data preparation and text representation techniques have been conducted. The results indicate a notable improvement in the accuracy of the online machine learning classifier PAC compared with conventional machine learning algorithms. The results also showed the effectiveness of the Bi-GRU with attention model and its superiority over all models used in classifying hate speech in the Arabic language. For upcoming plans, we plan to assess the effects of various contextualized word embedding techniques (e.g., BERT, GPT, GPT-2, and Elmo) on hate speech models. Another area of future work is to look into recognizing other types of harmful information on social media, such as video or audio with hateful speech.

Acknowledgements The authors would like to thank **Dr. Ahmed Omar**, From Computer Science Department, Faculty of Science, Minia University, for his support in providing us with the dataset.

References

1. Cortis K, Davis B (2020) Over a decade of social opinion mining. Springer, Netherlands. https://doi.org/10.1007/s10462-021-10030-2
2. Aljarah I, Habib M, Hijazi N, Faris H, Qaddoura R, Hammo B, Abushariah M, Alfawareh M (2020) Intelligent detection of hate speech in Arabic social network: a machine learning approach. J Inf Sci. https://doi.org/10.1177/0165551520917651
3. Jahan MS, Oussalah M (2021) A systematic review of Hate Speech automatic detection using Natural Language Processing (2021)
4. Salminen J, Hopf M, Chowdhury SA, Jung S, gyo, Almerekhi H, Jansen BJ (2020) Developing an online hate classifier for multiple social media platforms. Human-centric Comput Inf Sci 10:1–34. https://doi.org/10.1186/s13673-019-0205-6
5. Omar A, Mahmoud TM (2020) Comparative performance of machine learning and deep learning algorithms for Arabic Hate Speech detection in OSNs comparative performance of machine learning and deep learning algorithms for Arabic Hate Speech detection in OSNs. Springer International Publishing. https://doi.org/10.1007/978-3-030-44289-7
6. Husain F, Uzuner O (2021) A survey of offensive language detection for the Arabic Language. ACM Trans Asian Low-Resour Lang Inf Process 20:1–44. https://doi.org/10.1145/3421504
7. Abuzayed A, Elsayed T (2020) Quick and simple approach for detecting Hate Speech in Arabic Tweets. In: Proceedings of the 4th workshop on open-source Arabic Corpora and processing tools, with a shared task on offensive language detection, pp 109–114
8. Al-Hassan A, Al-Dossari H (2021) Detection of hate speech in Arabic tweets using deep learning. Multim Syst. https://doi.org/10.1007/s00530-020-00742-w
9. Hegazi MO, Al-Dossari Y, Al-Yahy A, Al-Sumari A, Hilal A (2021) Preprocessing Arabic text on social media. Heliyon. 7:e06191. https://doi.org/10.1016/j.heliyon.2021.e06191
10. Faris H, Aljarah I, Habib M, Castillo PA (2020) Hate speech detection using word embedding and deep learning in the Arabic Language Context Hate Speech detection using word embedding and deep learning in the Arabic Language context. https://doi.org/10.5220/0008954004530460
11. Al-Hassan A, Al-Dossari H (2019) Detection of hate speech in social networks: a survey on multilingual corpus, pp 83–100. https://doi.org/10.5121/csit.2019.90208
12. Haddad H, Mulki H, Oueslati A (2019) T-HSAB: A Tunisian Hate Speech and abusive dataset. Commun Comput Inf Sci 1108:251–263. https://doi.org/10.1007/978-3-030-32959-4_18

13. Mulki H, Haddad H, Bechikh Ali C, Alshabani H (2019) L-HSAB: a Levantine Twitter dataset for hate speech and abusive language, pp 111–118. https://doi.org/10.18653/v1/w19-3512
14. Albadi N, Kurdi M, Mishra S (2018) Are they our brothers? Analysis and detection of religious hate speech in the Arabic Twittersphere. In: Proceedings of the 2018 IEEE/ACM international conference on advances in social networks analysis and mining, ASONAM 2018, pp 69–76. https://doi.org/10.1109/ASONAM.2018.8508247
15. Elmadany A, Zhang C, Abdul-Mageed M, Hashemi A (2020) Leveraging affective bidirectional transformers for offensive language detection, pp 102–108
16. Mubarak H, Darwish K, Magdy W, Elsayed T, Al-Khalifa H (2020) Overview of {OSACT}4 {A}rabic offensive language detection shared task. In: Proceedings of the 4th workshop on open-source Arabic Corpora and processing tools, with a shared task on offensive language detection, pp 48–52
17. Hassan S, Samih Y, Mubarak H, Abdelali A, Rashed A, Chowdhury S (2020) ALT submission for OSACT shared task on offensive language detection, pp 61–65
18. Elzayady H, Badran KM, Salama GI (2019) Sentiment analysis on Twitter Data using Apache spark framework. In: Proceedings—2018 13th international conference on computer engineering and systems, ICCES 2018, pp 171–176. https://doi.org/10.1109/ICCES.2018.8639195
19. Gupta S, Meel P Passive-aggressive classifier. Springer, Singapore. https://doi.org/10.1007/978-981-15-7345-3
20. Nagashri K, Sangeetha J Passive-aggressive classifier and other machine learning algorithms. Springer, Singapore. https://doi.org/10.1007/978-981-33-6987-0
21. Li P, Luo A, Liu J, Wang Y, Zhu J, Deng Y, Zhang J (2020) Bidirectional gated recurrent unit neural network for Chinese address element segmentation. ISPRS Int J Geo-Information 9. https://doi.org/10.3390/ijgi9110635
22. Tay NC, Tee C, Ong TS, Teh PS (2019) Abnormal Behavior recognition using CNN-LSTM with attention mechanism. In: 2019 IEEE international conference on electrical, control and instrumentation engineering, ICECIE 2019—proceedings. https://doi.org/10.1109/ICECIE47765.2019.8974824
23. Haddad B, Orabe Z, Al-Abood A, Ghneim N (2020) {A}rabic offensive language detection with attention-based deep neural networks. In: Proceedings of the 4th workshop on open-source Arabic Corpora and processing tools, with a shared task on offensive language detection, pp 76–81
24. Mohaouchane H, Mourhir A, Nikolov NS (2019) Detecting offensive language on Arabic social media using deep learning. In: 2019 6th International conference on social networks analysis, management and security, SNAMS 2019, pp 466–471. https://doi.org/10.1109/SNAMS.2019.8931839

Application of Fuzzy Logic in Sales Inventory System: A Literature Review

Gede Indrawan, I. Putu Andika Subagya Putra,
Luh Joni Erawati Dewi, and I. Gede Aris Gunadi

Abstract The largest revenue comes from most sales. If the company offers far fewer types of goods than the types demanded, the company loses the opportunity to generate maximum revenue and vice versa. Therefore, planning the number of product purchases for inventory becomes very important. The purpose of this study is to review what factors cause inventory to increase. The literature review is primarily based on questions, methodologies, similarities, and additional research suggestions. This study uses seven papers including using the fuzzy method for inventory in sales. Based on the results of those papers, the fulfillment of inventory prices built by fuzzy logic will help to understand the purchase of various products in inventory in the next month. The analysis found that the inventory that is close to optimal is obtained through calculations using the fuzzy method.

Keywords Fuzzy logic · Sales inventory · Company product

1 Introduction

With the advancement of technology, many ways have evolved to deliver products. The amount of product made is inspired by several factors, including fee factor, number of workers, transportation, manufacturing method, demand, inventory level, and various items that the company wants to provide the product. Production systems with limited resources limit control opportunities and uptime delays response [1]. The industry needs to control its production costs. To increase profit and reduce the prices within the competitive environment, corporations face such a large amount of challenges in Supply Chain Management (SCM) [2]. Inventory allocation decisions in a distribution system concern issues such as how much and where the stock should be given to orders in a supply chain [3]. Various types of methods can be used to determine how much product is manufactured, for example, using the fuzzy method. Fuzzy logic is a mathematical term that is observed by many researchers in different

G. Indrawan (✉) · I. Putu Andika Subagya Putra · L. J. E. Dewi · I. Gede Aris Gunadi
Universitas Pendidikan Ganesha, Singaraja, Bali 81116, Indonesia
e-mail: gindrawan@undiksha.ac.id

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_47

fields during different time periods [4]. Fuzzy logic is logic that is simple to know and very flexible since it can adapt to changes and the certainty that accompanies problems; therefore, it is applied to an application that will optimize inventory [5]. Fuzzy logic is also used as a solution to formulate classification problems in filling out an inventory [6]. The inventory control using the fuzzy set theory has distinct advantages in reducing the number of set-ups and stock-outs [7]. In general, fuzzy logic can be used to determine the production volume of a product. Specifically, there are three techniques available, namely Tsukamoto, Mamdani, and Sugeno [8]. Tsukamoto technique is divided into four stages: fuzzification, rule formation, rule evaluation with the most implication feature method, and non-fuzzy unification using a common weighted technique. Mamdani and Sugeno techniques have the same four levels, i.e., fuzzy, rule forming, rule evaluation using implication functions with MIN function (there are also rule composition process using MAX function), and defuzzification. In defuzzification process, Mamdani method uses the centroid technique, and Tsukamoto and Sugeno methods use centered average method.

Several sections compose this paper. The Introduction section explains behind the scenes the use of fuzzy logic to support companies in determining inventory. This section also describes some of the previous related research in this area. The Research Methods section includes determining which articles are selected for review. The Results and Discussion section analyzes the results of the seven selected paper reviews. The Conclusion section consists of several conclusions and suggestions.

2 Research Methods

This chapter discusses journal finding techniques used in the literature review, questions about conducting journal reviews according to keywords and search terms in journals through the methods used, and much more. The journals used for the literature evaluation were obtained from the university journal provider database through Google Scholar. The author opens the journal website. The author then selects a journal that is appropriate to the topic under study, and seven journals are selected for the author. Another applicative problem that the author uses is the company's inventory system journal applying fuzzy logic. The author uses all research designs used to identify factors that increase the optimization of product production.

3 Research Result

In the research conducted by K. Harefa, inventory can be a problem that is often faced by decision-makers in the industry [9]. The query structure is inherently irregular and needs to be stored. Inventory is distributed to confirm knowledge that this product will be available when needed. Inventory is the determination of the amount of inventory that must be provided to meet the amount of demand. Carrefour Puri Indah is one of the retailers who always have problems with their product inventory expertise. One of the common problems faced in this business is the amount of inventory that accumulates over time which causes build-up. In this example, the company's interest expense is high. In addition, when a product is out of stock, the company may lose the buyer's trust or switch to a similar product from another brand. To overcome this, it is necessary to analyze and process past sales transactions to determine the amount of inventory to determine the level of inventory that must be available and when to buy back to increase inventory. This is necessary to ensure the availability of the right inventory in the right quantity and time. This study uses the application of the Fuzzy Inference System method that can be used to determine the amount and when to purchase products for inventory. Fuzzy logic is considered to allow inputs to be mapped to outputs without ignoring the current factor. Fuzzy logic is considered versatile and has tolerance for existing data. With the help of fuzzy logic, a model is generated by the system that estimates product purchases for inventory. Factors that influence purchasing decisions of a product for inventory using fuzzy logic include inventory, sales, and purchases.

In a study conducted by L. Satya Application of the Fuzzy Mamdani Method for Decision Support in Determining the Amount of Production of Lantak Si Jimat. Fuzzy logic is a calculation method that is mainly based on the level of facts and is commonly referred to as real or false values / 1 or 0. Fuzzy logic is a "counting method" that uses variable words instead of numbers [10]. These studies were conducted using Mamdani fuzzy to predict the production of Lantak Si Jimat, predict production strongly, and complete the production calculation method. The advantage of using the fuzzy logic method is that it is easy to understand, flexible, can use rules as necessary, and has tolerance for inappropriate data.

Research conducted by Winarti [11], the decision support system when determining inventory uses fuzzy. This research method uses Fuzzy Tsukamoto. The results of this survey are aimed at facilitating the activities of kemilau shops in the demand for goods from suppliers and ensuring that shops can order goods properly.

Research conducted by Azizah, implementation of fuzzy logic on inventory optimization using the Mamdani method. To optimize the existing inventory at the Affan stall, fuzzy logic with the Mamdani method can be used. The use of fuzzy logic to optimize inventory at Affan stalls so that they are not overstocked. The research used the method of literature study and data analysis. Based on the inventory analysis, it can be concluded that the inventory of goods that are close to optimal is determined by calculations using the Mamdani fuzzy method. The results of data accuracy are done manually or using MATLAB which is 83.3% [12].

Research conducted by Alfannisa Annurullah Fajrin, Optimizing product inventory and order quantity with fuzzy logic at PT. Hilti Nusantara Batam. The method used is the Mamdani fuzzy method known as the Min–Max method, by finding the minimum load for each rule and the maximum load for the mixed effect of each rule. This technique was added by Ebrahim H. Mamdani in 1975. The Mamdani technique is appropriate as long as the input is taken by humans rather than machines. This method is more general than the Tsukamoto and Sugeno methods. The usefulness of the Fuzzy Inference System in the Mamdani method in the system created can increase efficiency in the number of orders, which with more efficient orders can affect the price of goods and the value of warehouse inventory as well as a more measurable time period at PT Hilti Nusantara Batam [13].

Research conducted by Billy Chrisdianta Kosasih, Decision Support System with Tsukamoto fuzzy logic (Case study: Kencana Photo Studio), fuzzy logic is a suitable method for mapping the input space to the output space. Fuzzy logic was first introduced in 1965 by Professor Lotfi Zadeh. The Tsukamoto method is an extension of the monotonous way of thinking. In Tsukamoto's method, each sequence of IF–Then rules must be represented by a fuzzy set with a monotonic membership function. As a result, the inference output of each rule is scored explicitly (crisp) based on a-predicate (fire strength). Based on the research conducted, it can be concluded that the decision support system uses logic to determine the order of goods. Fuzzy Tsukamoto can assist the decision-making process of Kencana Photo Studio owners by providing recommendations on how to determine the number of orders [14].

Research conducted by Julio Warmansyah, the application of the fuzzy Sugeno method for prediction of raw material inventory. This research is using the fuzzy Sugeno method which can help in predicting the inventory of raw materials, so this prediction can determine the output, namely the amount of the final stock, to support the smooth production and gain profit for the company. After applying the fuzzy Sugeno method in determining the ending stock for optimal prediction of raw materials inventory, it can be concluded as follows: 1. Found a method that can predict raw material inventory using the fuzzy Sugeno method. 2. Obtain the optimal amount of final stock to be used as raw material inventory in the next period. 3. Prediction results of raw material inventory using the fuzzy Sugeno method get a MAPE value of 38% [15]. According to the prediction evaluation table, the value of 38% is included in the Reasonable assessment (Table 1).

4 Conclusions and Suggestions

The fuzzy logic approach can be used to anticipate the ups and downs of a company's production by calculating raw materials for production so as to get the optimal amount of final stock to be used as raw material inventory in the next period. From the manual calculations that have been done which are discussed with the results obtained using MATLAB, the results are close to accurate.

Table 1 Literature Review 7 Journal Fuzzy Logic

Title	Method	Research result
Application of Fuzzy Inference System to Determine Number of Product Purchases Based on Inventory and Sales Data [9]	Fuzzy Inference System on data processing of product purchases for inventory using the fuzzy Mamdani method	Based on the components of the problem, the effects of studies, and dialogue on figuring out the number of product purchases primarily based totally on stock and sales records, numerous conclusions may be drawn, namely: Fuzzy logic (Mamdani) in figuring out the number of product purchases for inventories that have been constructed may be used to help groups in making selections with a fact cost attaining 44.49656% for records testing Fuzzy logic (Mamdani) that has been constructed can assist Carrefour in figuring out the number of product purchases for stock in the following month
Application of the Fuzzy Mamdani Method for Decision Support in Determining the Amount of Production of Lantak Si Jimat [10]	Fuzzy logic is a method of computing primarily based totally on ranges of fact which can be normally said to be authentic or false/1 or 0. Fuzzy good judgment is a “counting” technique with variable words, in place of counting with numbers	This study was conducted to obtain the best prediction of the total production of Lantak Si Jimat, to obtain a strong prediction of the amount of production, the procedure for calculating the amount of production was completed using a good Mamdani fuzzy assessment technique. The benefits of using this assessment technique are that the idea is easy to understand, flexible, can use guidelines as important and displays a tolerance for irrelevant data
The decision support system in determining stock of goods using fuzzy [11]	The method in this study makes use of fuzzy Tsukamoto	The results of this study are to facilitate the activities of the kemilau shop in the demand for goods to suppliers so that the stores can order goods properly

(continued)

Table 1 (continued)

Title	Method	Research result
Implementation of Fuzzy Logic in Optimizing Goods Inventory Using the Mamdani Method [12]	To optimize the existing inventory at the Affan stall, fuzzy logic with the Mamdani method can be used. The use of fuzzy logic is needed to optimize the inventory of goods at Affan's stalls so that the inventory is not excessive. The research method uses the method of literature study and data analysis	Based on data analysis, it can be concluded that the most effective stock is obtained by calculating the use of the Mamdani method. The consequence of recording accuracy that is done manually or using MATLAB is 83.3%
Optimization of Product Inventory and Order Quantity with Fuzzy Logic at PT. Hilti Nusantara Batam [13]	The approach used is the Mamdani approach, called the Min–Max approach, through locating the minimal cost of every rule and the most cost of the combined outcomes of every rule. This approach changed into added through Ebrahim H. Mamdani in 1975	The application of the Mamdani Fuzzy Inference System on the system created can increase efficiency in the number of orders, which with more efficient orders can affect the price of goods and the value of warehouse inventory as well as a longer period of time at PT Hilti Nusantara Batam
Decision Support System For Determining Goods' Order Using Tsukamoto Fuzzy Logic (Case Study: Studio Foto Kencana) [14]	The application uses the Tsukamoto method which is used to analyze input data to get a decision	Based on the research that has been done, it can be concluded that the selection tool for determining the order of goods using Fuzzy Tsukamoto logic can assist in the selection of Kencana Photo Studio owners in providing instructions for determining variations of the order
The application of the Sugeno fuzzy method for prediction of raw material inventory [15]	This research is using the fuzzy Sugeno method that can help in predicting the inventory of raw materials, so this prediction can determine the output, namely the amount of the final stock	After applying the fuzzy Sugeno method in finding the ending inventory for the ideal prediction of the optimal raw fabric stock to be used as raw material inventory in the next period

References

1. Suhail A, Khan ZA (2005) Fuzzy control with limited control opportunities and response delay—a production-inventory control scenario. Int J Approximate Reasoning 38(1):113–131
2. Sona P, Johnson T, Vijayalakshmi C (2018) Design of an inventory model - fuzzy logic controller approach. International Journal of Pure and Applied Mathematics 119:41–51
3. Wanke P, Alvarenga H, Correa H, Hadi-Vencheh A, Azad MAK (2017) Fuzzy inference systems and inventory allocation decisions: Exploring the impact of priority rules on total costs and service levels. Expert Syst Appl 85:182–193
4. Renu, M.: Application of fuzzy logic: A literature review. International Journal of Statistics and Applied Mathematics, 357–359 (2018).
5. Riyanto, A., Marcos, H., Karini, Z., Amin, K. M.: Fuzzy logic implementation to optimize multiple inventories on micro small medium enterprises using mamdani method (Case Study: Pekanita, Kroya, Cilacap). In: International conferences on Information Technology, Information Systems and Electrical Engineering (2017).
6. Yung KL, Ho GTS, Tang YM, Ip WH (2021) Inventory classification system in space mission component replenishment using multi-attribute fuzzy ABC classification. Ind Manag Data Syst 121(3):637–656
7. Lakshmi MD, Pandian P (2018) A Review on Inventory Models in Fuzzy Environment. International Journal of Pure and Applied Mathematics 119:113–123
8. Setiadji: Fuzzy Set and Logic with Applications [Himpunan dan Logika Samar serta Aplikasinya]. Yogyakarta: Graha Ilmu (2009).
9. Harefa K (2017) Application of the Fuzzy Inference System to Determine the Number of Product Purchases Based on Inventory and Sales Data [Penerapan Fuzzy Inference System Untuk Menentukan Jumlah Pembelian Produk Berdasarkan Data Persediaan Dan Penjualan]. Jurnal Informatika Universitas Pamulang 2:205–213
10. Satya, L., Mifah M., Saepudin S., Mandala V., Gustian D.: Application of the Fuzzy Mamdani Method for Decision Support in Determining the Amount of Production of Lantak Si Jimat [Penerapan Metode Fuzzy Mamdani Untuk Pendukung Keputusan Penentuan Jumlah Produksi Lantak Si Jimat]. Jurnal Rekayasa Teknologi Nusa Putra 4, 2017.
11. Winarti W, Gustianty G (2019) Decision support system in determining stock of goods using fuzzy [Sistem pendukung keputusan dalam menentukan stock barang menggunakan fuzzy}. Jurnal Aplikasi Teknologi Komputer dan Informasi 1:115–120
12. Azizah A, Kasyfi F (2020) Implementation of Fuzzy Logic in Optimizing Goods Inventory Using the Mamdani Method [Implementasi Logika Fuzzy Dalam Mengoptimalkan Persediaan Barang Dengan Metode Mamdani]. Satuan Tulisan Riset dan Inovasi Teknologi 5:20–27
13. Fajrin, A. A.: Optimization of Product Inventory and Order Quantity with Fuzzy logic at PT. Hilti Nusantara Batam [Optimasi Inventory Produk dan Jumlah Pesanan dengan Fuzzylogic pada PT. Hilti Nusantara Batam]. Jurnal Edukasi dan Penelitian Informatika 3, 134–141 (2017).
14. Kosasih BC, Setiyawati N (2020) Decision Support System For Determining Goods' Order Using Tsukamoto Fuzzy Logic (Case Study: Studio Foto Kencana) [Sistem Pendukung Keputusan Penentuan Pemesanan Barang Menggunakan Logika Fuzzy Tsukamoto (Studi Kasus: Studio Foto Kencana)]. Jurnal Algoritma, Logika dan Komputasi 3:215–222
15. Warmansyah J, Hilpiah D (2019) The application of the Sugeno fuzzy method for prediction of raw material inventory [Penerapan metode fuzzy sugeno untuk prediksi persediaan bahan baku]. Jurnal Ilmiah Teknologi Informasi dan Sains 9:12–20

Statement Emotion Decision Model for Human-Friendly Chatbot

Kyoungil Yoon, HeeSeok Choi, and Kwang Sik Chung

Abstract A chatbot is a software that gives proper answers and information for users, and provides useful information to users. Users basically express their feelings to others, and seek to exchange their feelings. However, the chatbot does not respond to the user's emotional state, but focuses on providing information. Since the chatbot understands the intention of the question without considering the user's emotional state, the accuracy of intention analysis is poor, and cannot provide accurate answers. In this paper, we develop a module that can know the user's mood, including newly coined terms and emojis, and apply it to the chatbot. The chatbot consists of an intent decision module that analyzes the user's intention, a mood decision module that infers the user's internal mood, and an answer decision module that generates answers to the user's sentences. The mood decision module consists of an emotion classification model that classifies the user's emotions through the sentences of users, and a mood determination model that infers the user's mood through the classified emotions. It infers the user's current mood state in real-time using the emotion classification model and the mood determination model. The chatbot analyzes morphemes and syntax for user sentences. By building a sentiment dictionary based on the Korean dictionary, the emotions of morpheme-analyzed words are classified. To classify the emotions of new words and emojis, the newly coined terms and emojis emotion dictionary is used to classify the emotions of newly coined terms and emojis. Emotions are classified using naive Bayes classification, and for words that are not classified by naive Bayes classification, an artificial neural network model is used to increase the accuracy of emotion classification. The chatbot infers the mood state using the mood determination model. The mood state consists of the emotional state representing the

K. Yoon
Graduate School, Dept. of Information Science, Korea National Open University, Seoul, Korea
e-mail: pofour@knou.ac.kr

H. Choi
ATGLab R&D Center, Seoul, Korea
e-mail: hs.choi@atglab.co.kr

K. S. Chung (✉)
Department of Computer Science, Korea National Open University, Seoul, Korea
e-mail: kchung0825@knou.ac.kr

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_48

eight emotions to be classified and each emotional value, and infers the user's mood with the mood state extracted through the mood determination process.

Keywords Emotion classification · Mood determination · Chatbot

1 Introduction

The chatbot is a compound word of bot and chat, and is a software that gives answers and information for user. A chatbot refers to 'artificial intelligence-based communication software' that responds through text conversations with people, and provides appropriate answers to questions or various related information [2]. In general, a chatbot can be classified as a rule-based chatbot or an emotion model based chatbot, according to the user's input and emotion classification. Whereas the rule-based chatbot does not classify emotion, an emotion model based chatbot does. The rule-based chatbots are chatbots used in the past, and operate according to predefined rules. They contain an interpretation rule that interprets the user's input, a reaction rule that reacts to the input, and a response rule. The development of rule-based chatbots does not require a large amount of data, and is relatively easy to implement. If the rules are well defined, a high-quality dialogue service is possible. However, defining the rules for smooth conversation requires a lot of time and manpower.

To solve this problem, [3] developed a chatbot based on an emotion model. The authors classified emotions into three categories: joy, sadness, and anger, through the sentences input by the user. However, newly coined terms and emojis were excluded from sentiment analysis. Internet terms are newly coined terms, are used both within the Internet and in the real world, and have several characteristics. First, most of the newly coined terms are rapidly made or disappear according to fashion. Second, these newly coined terms have no standardized and normalized corpus, so it is difficult to analyze the meaning of the word, or the emotion contained therein. Finally, newly coined terms and emojis are easily and always used in internet SNS or chats, and connote certain emotions and intentions. In other words, the exclusion of newly coined terms and emojis from emotional analysis causes inaccuracy of emotion analysis, and therefore could potentially misinterpret the user's emotional state.

2 Related Works

Table 1 lists the methods for classifying subdivided emotions in Korea. Domestic studies on identifying and classifying subdivided emotions are insufficient, compared to overseas studies. Existing studies conducted a study to classify emotions in sentences through various classification methods. Various classification algorithms were used and a study was conducted to classify many kinds of emotions, but emotion classification for newly coined terms and emojis was not performed [4–7]. In this

Table 1 Table captions should be placed above the tables [3]

Reference	Number and list of emotional categories	Classification method
Yun-Suk Kim [4]	9 (Joy, Surprise, Interest, Fear, Anger, Disgust, Pain, Boredom, Sadness)	SVM
Myung-Kyu Kim [5]	10 (Joy, Reassurance, Satisfaction, Fun, Pride, Anger, Fear, Disgust, Dissatisfaction, Sadness)	Statistical method
Cheol-seong Lee [6]	7 (Anger, Confusion, Depression, Fatigue, Intimacy, Tension, Vitality)	Bayesian probability model
Young-hee Jung [7]	25 (Joy, Fun, Pleasure, Gratitude, Love, Sadness, Regret, Fear, Regret, Depression, …)	SVM, linear regression

paper, the criteria for classifying the eight emotion categories of joy, sadness, trust, anger, fear, expectation, surprise, and displeasure are based on emotional wheel techniques [8]. The reason for using eight emotion categories is that eight emotions can best express the representative emotions that people feel as much as possible. In addition, it is easy to expand the emotional category, as it defines the emotions that appear in a mixture of eight emotions. In SNS or Internet environment, users convey feelings and intentions in their sentences. In particular, they use only newly coined terms and emojis to convey their feelings and intentions implicitly.

Unlike existing research, we applied newly coined terms that can express users' emotions as research subjects to improve emotion analysis accuracy. Since the newly coined terms frequently used on Internet are not listed in the dictionary, when morpheme analysis is performed based on the Korean dictionary, the newly coined terms do not have any form of part-of-speech. In addition, it is difficult to construct a corpus, since the fleeting nature of the newly coined terms that are easily created, and then easily disappear. Hence, a corpus of meanings and emotions expressed by newly coined terms and emojis mainly used on the Internet is constructed. Expression of emotions using newly coined terms and emojis is more common than expressing emotions through sentences, and the accuracy of emotion classification can be improved by analyzing newly coined terms and emojis. In this paper, image-type emoticons are excluded from the dictionary of new words and emojis of [1]. And the emotions expressed by the new words and emojis were classified into eight emotional states. The newly coined term and emoji emotion dictionary was constructed by tagging the classified newly coined terms and emotional states of emojis.

In this paper, we apply emotion classify model for newly coined terms and emojis to the standard word-based emotion classification method to increase the accuracy of emotion classification in a mobile chatting environment. We design newly coined terms and emojis by excluding image-type emojis in an efficient way. In addition, [2] used the Emotion–Mood emotion model excluding Personality and Feeling from the Emotion–Mood–Personality emotion model. This is conducted to immediately classify emotions by reducing the variables that determine emotions in environments such as mobile chatting.

3 Statement Emotion Decision Model Design

3.1 Mood Decision Module Design

We define the emotion that users feel through the use of morphemes, words, newly coined terms, and emojis as emotional states. Moreover, the intensity of each emotional state is quantified and defined as the emotional value. A dictionary of newly coined terms and emojis is built based on newly coined terms and emojis that represent human emotions, and a dictionary-based emotion dictionary of Korean is also built based on morphemes and words defined in the Korean dictionary. Emotional classification uses an emotional dictionary that includes eight emotions (joy, sadness, trust, anger, fear, hope, surprise, and displeasure), referring to Plutchick's emotional wheel [8]. However, our proposed dictionary of newly coined terms and emojis refers to the techniques in [4, 9], constructed by extending the emotional state excluding image-type emojis. The Korean dictionary-based emotion dictionary is constructed by extending the emotional state by referring to the polarity values in [10].

Newly coined terms and emojis are not listed in the Korean dictionary, and during morpheme analysis are not recognized as morphemes, we divide into word units and compare. The emotion extraction model determines the emotional state of the newly coined term and emoji when the one word is registered in the newly coined term and emoji dictionary. To classify the emotions of newly coined terms and emojis that do not exist in the dictionary, the model is trained using the Naive Bayes method. In addition, we train using the word2vec model, which is trained using dataset provided by AI-Hub. The trained model determines the emotional state of newly coined terms and emojis that do not exist in the emotion dictionary by using newly coined terms and emojis whose emotional state is determined. Then, newly coined terms and emojis, whose emotional state is determined by the manager, are added to the dictionary of newly coined terms and emojis. Moreover, the Korean dictionary-based emotion classification compares the Korean dictionary-based emotion dictionary with the morpheme, to determine the emotional state of the morpheme. The operation of the emotion extraction model to determine the emotional state of the morpheme is the same as the operation for determining the emotional state of the newly coined terms and emoji.

In other words, the emotion extraction model finally determines the emotional state of the user's sentence by the emotional state of newly coined terms and emojis with the emotional state of morphemes. The determined emotional state is updated for the emotion column of the input table, and the emotional state of the user's sentence is used as input of the mood determination model. After that, in the mood determination model, the user calculates the user's mood state of the conversation based on the emotional states of the input sentences. The mood state represents a value that infers the emotion the user is currently feeling.

Mood determination model. Figure 1 shows that the mood determination model determines the 'mood state' that infers the user's mood.

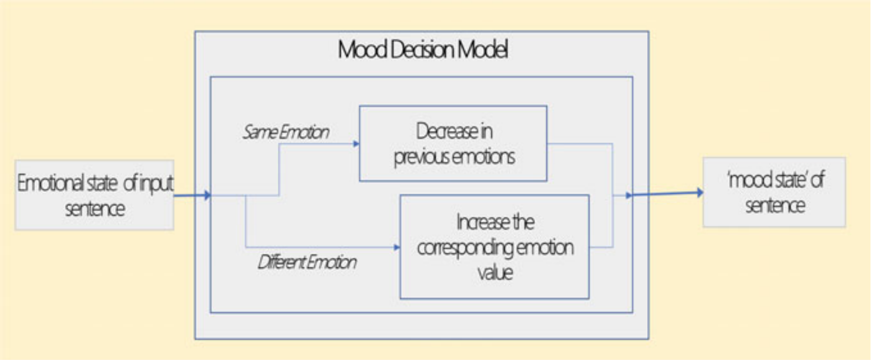

Mood Decision Model
Emotional state of input sentence
Same Emotion
Decrease in previous emotions
Different Emotion
Increase the corresponding emotion value
'mood state' of sentence

Fig. 1 Mood determination model

A 'mood state' consists of an emotional state having one of eight emotions and the accumulated values of the emotional state. The minimum value of emotion value is 0. The mood determination model uses the emotional state of the sentence extracted from the emotion extraction model as an input value, and when the emotional state of a sentence is input to the mood determination model, it is compared with the emotional state of the previous sentence to check whether the emotional state is the same.

If the same emotional state is continuously input, we determine that the user feels the corresponding emotion strongly, and increase the emotion value by 2 for the input emotional state. On the other hand, if the same emotional state is not continuously input, we set the emotional value corresponding to the input emotional state by 1. Additionally, when a sentence is input, the emotion value of the previous input sentence is decreased by 0.1 to express the feeling that the user's emotion weakens over time. Table 2 shows the changes in emotion value according to the order of emotional state input:

Table 2 An illustrative example of the mood determination model operation

		When entering the first 'joy'	When entering the second 'sadness'	When entering the third 'sadness'
Mood	Joy	1.0	0.9	0.8
	Sadness	0	1.0	2.9
	Trust	0	0	0
	Anger	0	0	0
	Fear	0	0	0
	Expectation	0	0	0
	Surprise	0	0	0
	Displeasure	0	0	0

Table 3 Results of emotion tagging of the Sejong Corpus

Emotion category	Count	Emotion category	Count
Joy	1839	Sadness	3359
Surprise	501	Angry	2914
Trust	1100	Fear	1835
Expectation	1657	Displeasure	2649

We set the corresponding emotional state to (weak) if the accumulated emotional value is from 0.4 to <3.5, and set the corresponding emotional state to (strong) if it is $\geq$3.5. The proposed method prioritizes strong emotional states to determine 'mood states.' When there are two or more strong emotional states, the mood determination model compares the accumulated emotional values of the strong emotional states, and determines the 'mood state' as the emotional state with the larger emotional value. Even when there is no strong emotional state and there are two or more weak emotional states, the mood determination model determines the 'mood state' by comparing the accumulated emotional values in the same way as when there are two or more strong emotional states. In addition, when the accumulated emotional value of all emotional states is $\leq$0.4, 'stability' is output to express a neutral mood that is not biased by any emotion. The proposed approach updates the 'mood state' whenever the user inputs a sentence.

3.2 Development

Development environment. In this section, we present an experimental setup that demonstrates the performance of the emotion model in terms of increasing the accuracy by classifying emotion and predicting the user's mood.

The morpheme analyzer is compared to the Kokoma morpheme analyzer and the Komoran morpheme analyzer. When analyzing sentences that complied with spacing, the two morpheme analyzers showed similar performance. However, when comparing sentences that did not comply with spacing, the Kocoma morpheme analyzer performed detailed morphological analysis including investigation. As a result, since the characteristics of the mobile environment input are that spacing and grammar are not well observed, the accuracy of morpheme analysis is improved by using the Kocoma morpheme analyzer.

Database configuration. The user input table is a table that stores the sentences input by the user. The similar/synonym table is a table for substituting representative words for several words with similar meanings to analyze the intent of a sentence. The intent table is a table for extracting the intent indicated by each word. As a table for emotion analysis, an emotion tagging table based on the Sejong Corpus is constructed (emotion_sejong). The Sejong Corpus emotion table uses the word for each morpheme, the morph to indicate the type of morpheme, and the emotion_value column for the emotional state. Table 3 lists the number of tags by emotion classification:

Naive Bayes classification. Eight emotions are tagged for 89,578 common nouns and 23,085 verbs of the Sejong Corpus. The tagged morphemes are 1325 common nouns and 14,529 verbs, for a total of 15,854, and the morpheme and the emotional state in the Korean dictionary-based emotion table. At this stage, the eight emotions are joy, trust, hope, surprise, sadness, anger, fear, and displeasure. The Naive Bayes classification method is used by applying the emotion-tagged morphemes. In addition, the user's sentence is morphologically analyzed and separated into morpheme units. The separated morphemes use the Naive Bayes classification method to extract the emotional state of the morpheme that has an emotional state.

word2vec different results are obtained, depending on the corpus used to build the model. When the word 'happiness' is input, love, joy, and pleasure are output as nearby. In contrast, when 'sad' is input, 'joy' is output as the closest value. This is because joy and sadness are frequently used together in the corpus used to build the model, and are located in a nearby vector space.

Auto-tagging of newly coined terms and emojis. To increase the accuracy of emotion classification, it is necessary to constantly update tagged emotions, but it is very difficult to continuously update newly coined terms and emojis that appear and disappear quickly. Therefore, we need a solution for automatically tagging newly coined terms and emojis that do not exist in the dictionary of newly coined terms and emojis. The newly coined terms and emojis are mainly used to emphasize a user's specific emotion or intention in a sentence of a conversation. Thus, newly coined terms and emojis that are opposite to the emotions appearing in the sentence are not used. We add eight emotions that need to be classified for each newly coined term and emoji as a column in the newly coined term and emoji dictionary. The emotions, in which the user sentences that include the newly coined terms and emojis are classified, are used to update the emotion values indicated by the newly coined terms and the emojis. By performing batch processing, the counts of the eight emotion columns of the newly coined term and emoji dictionary are automatically compared, and the emotion expressed by the corresponding newly coined term and emoji is updated with the emotion with the highest count. Newly coined terms and emojis are not used for emotion classification, and they have the overall emotional state represented by the sentence. When a newly coined term and an emoji are used alone, they have the emotion expressed in the mood state extracted by the mood determination model.

4 Conclusion

In this paper, we propose an algorithm for subdividing the emotion classification of input sentences and user's mood prediction, and an emotion model that can classify eight emotions. A Korean dictionary-based emotion dictionary is constructed by tagging eight emotions to words and verbs used to express human emotions in the Sejong Corpus. To classify the emotions expressed by newly coined terms and emojis in user sentences, eight kinds of emotional states are tagged in existing newly coined term and emoji dictionary to expand the newly coined term and emoji emotion dictionary.

To increase the accuracy of emotion classification, newly coined terms and emojis used online are added to the subject of emotion classification. Emotion classification of input sentences is performed using Naive Bayes classification and word2vec. Unlike existing research, our method increases the accuracy of emotion classification of sentences containing newly coined terms and emojis.

As future work, we intend to upgrade the emotion model to classify the categories of emotions that are synthesized from different emotions based on the eight emotions. In addition, we will conduct research to improve user satisfaction by automatically generating a response that matches the predicted user's mood.

References

1. Yang JS (2020) Automatic newly-coined words and emoticons emotional dictionary construction and opinion mining based on sentiment sentence, Korea National Open University, Seoul
2. Lee SM (2018) A study on the implementation of a chatbot based on an emotion model. Domestic Master's Thesis Soongsil University Graduate School of Software Specialization, Seoul.
3. Kim MG, Cho DG, Kim HW (2017) Generative model chatbot technology analysis based on neural network. J Korean Inst Commun Sci 211–212
4. Kim YS, Seo YH (2013) Korean text sentiment classification using machine learning. J Korea Entertain Indus Assoc206–210
5. Kim MK, Kim JH, Cha MH, Chae SH (2009) An emotion scanning system on text documents. Korean J Sci Emotion Sensibility 12(4):433–442
6. Lee C-S, Choi D-H, Kim S-S, Kang J-W (2013) Classification and analysis of emotion in Korean microblog texts. J KIISE: Databases 40(3):159–167
7. Jung HY (2017) Study on machine learning based korean emotions classification methods, Ph.D. Thesis, Korea University
8. Plutchik R (2001) The Nature of Emotions: Human emotions have deep evolutionary roots, a fact that may explain their complexity and provide tools for clinical practice. Am Sci 89(4):344–350
9. Yoon K, Kang J, Chung KS (2021) Intelligent chatbot based on emotional model including newly-coined word and emoticons. Adv Intell Syst Comput 1363. https://doi.org/10.1007/978-3-030-73100-7_75
10. Github, https://github.com/coolengineer/sejong-corpus. Last accessed 24 Oct 2021

Secured Supercomputer Technologies in Russia: Functional Computing Units Based on Multithread-Stream Cores with Specialized Accelerators

Andrey S. Molyakov

Abstract A new direction in the design and implementation of Russian secure supercomputers is massively parallel reconfigurable computers. This article describes further development of secured strategic supercomputer "Angara." The service nodes are built on conventional superscalar microprocessors. Computing nodes are built on special multicore multithread-stream microprocessors (microprocessors of the J-series) are combined into modules in the form of multi-socket boards and can work on a logically single addressable memory (globally addressable memory). Author demonstrates basic features of new functional computing units with specialized accelerators.

Keywords Extremely productive systems · Data flow control · Specialized accelerators · Supercomputer "Angara"

1 Introduction

Russian strategic supercomputer "Angara" is a set of nodes of different types, united by several communication networks, one of which has a unique property of transmitting large streams of short packets with high throughput. This network is necessary to implement work with globally addressable memory; hereinafter, we will call it the basic working network (BNW-network). The nodes are connected to the basic working network and can be computing and service [1].

Computing nodes are built on special multicore multithread-stream microprocessors (microprocessors of the J-series) are combined into modules in the form of multi-socket boards and can work on a logically single addressable memory (globally addressable memory) formed by local memories of modules with computational nodes. There are two models of J-series microprocessors: The younger one is J7; the older one is J10. Further, the characteristics and principles of operation of the younger

A. S. Molyakov (✉)
Institute of IT and Cybersecurity, Russian State University for the Humanities, Moscow 125993, Russia
e-mail: andrei_molyakov@mail.ru

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_49

model J7 are considered; for the older model, a list of fundamental differences and general characteristics is given.

Service nodes are built on conventional superscalar microprocessors, perform the functions of input–output, user connection, interface with the global network, and can also perform computations if they are well localized and efficiently executed on these nodes. Computing and service nodes are connected to another network (RAS network), which is a component of the reliability, availability, and service subsystem. A detailed description of the system-wide specification can be found in publications [2, 3].

2 Methodology and Theoretical Approaches

The J7 microprocessor is referred to as a "multicore, multithread-stream microprocessor with support for globally addressable memory operations." The term "globally addressable memory" in the name of the microprocessor should be understood as follows: In the J7/J10 microprocessors, the virtual memory is organized so that when it is accessed, it is automatically recognized during the translation of the address which node of the system should be accessed, and this call is made without user intervention. The J7 microprocessor has two multi-threaded cores (MTcore0 and MTcore1). Four command pipelines are available in one multi-threaded core. Each of them works with 16 threaded devices, each of which can run one process [3]. Several tasks can be executed simultaneously in one microprocessor core. Each task is assigned one protection domain; one of the kernel tasks is the operating system. The user's task performed in the microprocessor can be simultaneously executed in the protection domains of its different cores; information about the task's binding to the protection domains is stored in a special table of the microprocessor.

The main idea behind hiding delays, i.e., ensuring its insensitivity to these delays in terms of the developed real performance—ensuring a high rate of execution of operations with memory and network. This requires a special organization of the processor and the applications running on it, a special organization of a communication network, and a special organization of memory. All of these devices require the ability to perform a large number of operations simultaneously and high pipelining. The computational model of the application is required to be able to issue a large number of operations, which is why multithreading is needed. Memory and network latencies can be up to ten-times higher; the pace is not always able to withstand the same operation per clock cycle, especially in the communication network—the physical limitations of the bandwidth of data transmission links between nodes within the network effect. For these reasons, a larger number of threaded devices are selected, up to 64–128 per MT core, which makes it possible to have up to 512–1024 concurrent memory or network accesses in one core. Commands of memory accesses are used behind short vectors, for example, up to 8 64-bit words, which increasing the number of concurrent memory accesses and reducing the overhead of organizing one memory access.

3 Multithread-Stream Cores with Specialized Accelerators

The term “streaming” is more applicable to the architecture of the J10 microprocessors and can be used in the sense of providing the ability to process data streams using data flow graph models. Two graph flow models are supported—static and dynamic graphs. These models are used to provide more parallelism and asynchrony, and static graphs are used to reduce the number of memory accesses when transferring data between nodes. A static graph node appears along with the entire graph, functions for some time, and then is deleted along with the graph. A node of a dynamic graph can appear and be destroyed during the operation of the graph. This possibility is preserved and strengthened in the Chinese version [4, 5, 15]. For a node of a dynamic graph, such a sequence of data arrival in an arc can be violated, so the data come with special tags, by the coincidence of which they can find a pair for themselves in the stream of another arc. The operation may be normal if there is a pair for which the operation can be performed. Such selection of data corresponding to each other in the streams of arcs requires the use of memory with associative access; in this case, the associative address is a data tag. Such memory is implemented in software. RPC commands are actively used in the implementation of dynamic graphs.

Technologies for creating supercomputers, including electronic components, in the last 10–15 years have been in demand in high-precision weapons systems and civilian products. The development of one or several options for replacing the GPU Volta (V100) was determined, which in domestic systems, due to its unique high performance, are used to solve problems from HPC to AI, but there is nothing to replace it. GPU Volta (V100) is powerful and extremely productive specialized processor. The lag behind domestic samples of universal and specialized processors in terms of capabilities for tasks from HPC is up to 30 times.

More detailed technical information about functional computing units based on multithread-stream cores with specialized accelerators can be found in articles [6–8]. The mt-LWP kernel contains four sections, each of which has 16 thread units (TUs) on which thread processes can run. Each TU is a set of general-purpose registers, thread local memory words, and thread system registers. The transition from the program executed on one TU to the program of another TU occurs without any overhead costs for memorizing/restoring program states. Each section contains the ALU section common to all TUs for performing simple arithmetic and logical operations, as well as a multiplier and a communication unit with the local LP memory. Switching between the executions of programs of different TUs is done in hardware either when there is a delay in the execution of a command on the TU or as a result of the execution of special commands for working with threads. TU sections interact with each other, as well as with the block of general special registers of the BOR, the SFU interface block through a one-cycle “bus” of inter-thread messages (MTS bus), implemented as a switch. In each section, work with the bus for receiving/issuing messages and performing special operations with the TU is performed by the BSO special operations units.

The main features of the mt-LWP kernel are as follows:

(a) 64-thread (thread) RISC processor: 32-bit and 16-bit signed integers, binary codes, bytes and bits, processing of floating-point numbers, and other data types in connected special devices—accelerators (SFU, their type is not fixed);
(b) 12 command formats, two of them are long format (32-bit); the rest are 16-bit; the number of commands is 141, of which 10 are long-format;
(c) In the program of each thread, the user has access to 8 32-bit general-purpose registers, with which you can work with both 16 16-bit registers, 32 words of superfast thread memory (LPT), several system registers;
(d) Commands of a thread are executed according to the "in-order" discipline; informational dependencies of commands are monitored by hardware; in one thread, it is possible to execute up to 8 memory accesses simultaneously; mt-LWP allows issuing up to 512 uncompleted memory accesses; in a thread, barrier synchronization is possible to complete the memory accesses issued by it;
(e) Hardware support for signal transmission, mailboxes with full/empty bits, implemented in words of superfast thread memory, barrier synchronization counters, atomic memory operations are available for thread interaction;
(f) Work with memory is provided in normal and extended mode, the main features: In normal mode, work is carried out on the local memory of a 256 KB tile through a 16-bit address, data addressing up to a 32-bit word, and commands—up to a half-word, if off-chip memory is connected, then a 32-bit address is used;
(g) Provides asynchronous transfer of blocks of different fixed lengths between local (off-chip) memory and memory accessible via GAS;
(h) Unified interface with SFU based on signaling is provided.

The interface for the interaction of threaded devices (TUs) with specialized functional units (SFUs) is based on the signaling means available in the TU.

4 Experimental Design Results

New principles of access security model are based on outbound command assembly and multi-domain protection. Given the development of vulnerability search methods, the implementation of reactive information protection methods should be considered, along with preventive ones. Instead of the classical concept of "localized task" for supercomputers (SC), one should speak of parallel distributed stream structures generated and processed at different levels of the command pipeline hierarchy by processor devices connected by high-speed networks.

Object access attributes and subject privileges, connections between them are formalized as a set (conjunction) of predicates. You can track interaction and control access by a set of characteristic features (markers), represented as tuples of Boolean variables. Information security is based on controlling access to objects of management and guest operating systems; these objects can be attributed to different levels of protection. The traditional approach to access control assumes the use of access attributes (rights) in requests to these objects to perform some operations on them. If the verification of such attributes is successful, then access to the object at its security level is allowed, then the requested operation is performed on it. With this approach, it is technically possible to intercept the request and use its access rights in a surrogate request aimed at malicious impact. We propose a new mathematical model for security. It is based on an 8-tier model (one level of protection was added) and new logic for controlling access to requests to perform actions with OS objects, which is implemented by a hypervisor with an appropriate organization, which additionally uses the architectural capabilities of the proposed supercomputer model extended by the author. In the course of experimental studies, new scientific results have been obtained that confirm the effectiveness and minimal loss of performance of the use of hardware virtualization technology in the form of a multi-level "sandbox" for promising SCs in comparison with the use of traditional superclusters. Since it is possible to control the execution of requests at the level of the components of the hypervisor and the transactional memory controller and it is impossible to control the operation of all equipment, during the research, the maximum level of functioning of the ISS agents was found—S8. With this configuration, when the number of levels of the hierarchy is $N = 8$, the execution of context-dependent operations becomes quasi-deterministic with a confidence level of approximately 0.9.

In classical processors with the von Neumann architecture, data and program codes are shared, which prevents the effective restriction of one object's access to the address space and data of another. They also do not implement multilayer protection mechanisms against attacks when executing system calls in a multi-level context of nested guest and control operating systems. Tagged architecture on the example of MCST Elbrus processor does not support hardware virtualization technology. However, the lack of support for hardware virtualization makes such architectural solutions highly specialized and does not support the emulation of various hardware and support for widely used hypervisors. Some features of the hardware virtualization technology also speed up the operation of virtual machines and increase the level of security. Hardware-assisted virtualization and multi-layered protection can reduce the overhead of creating an isolated runtime environment. In any operating system, when the kernel code is paired with hardware at the physical level, forbidden states appear—a zero tuple of data, which the processor prohibits accessing even programs in the zero protection ring. Only, the processor module can perform active task context switching in protected mode since when shadow copying the data of the executable code, the programmer cannot get direct access to the information. This requires the implementation of a tiered query-processing hierarchy.

This approach did not apply to previous generation microprocessors due to poor performance. The introduction of additional levels of privileges and levels of protection greatly slowed down the system as a whole [8, 9]. The high performance of supercomputers, on the contrary, makes it possible to quickly analyze descriptor tables and calculate hash values of processes. They are distinguished by self-diagnostics, multi-level protection, binding each thread device to a specific domain, programming using non-functional, non-procedural languages—chains of calculations in the form of selectors, substitutions on the right, left of functional calculations, multi-level parallelization of algorithms and etc. When the boot program is executed, the threading device operates in a special privilege mode—IPL_LEVEL. Physical addressing when accessing instruction memory and data memory is used in this mode, then the virtual infrastructure manager and host OSs with hypervisor support are loaded. In this case, the KERNEL_LEVEL level is used for the kernel modules and the SUPERVISOR_LEVEL level for the equipment manager. At the final stage, the guest OS is launched at the USER_LEVEL level. The only "stumbling block" in multicore multiprocessor systems is the problem of efficient implementation of the on-chip network and working with memory. The multicore microprocessors used in computational nodes have become a necessary measure to ensure the growth of their peak performance, and it is caused by the termination of the direct influence of Moore's law on the growth of processor cores performance. Multicore has given rise to the problem of efficient implementation of the on-chip network and exacerbated the problems of working with memory. Possible solutions include the use of multi-threaded and streaming architectures in processor cores.

The multithreading organization allows multiple threads of instructions to be executed concurrently, which makes it possible to increase the multitude of executable instructions and increase the flow of concurrent memory operations. The streaming architecture assumes the use of the decision fields of elementary processors in the form of static graphs of data streams. This makes it possible to reduce the total number of memory accesses since, in the decisive field, data are transferred from one fast resource to another without accessing memory [10]. The author proposes a method for reconfiguring the runtime environment, taking into account the requirements of mobility and ensuring the specific performance characteristics of the program for the safe expansion of the functionality of the system or application. Only, hardware support for sharded stacks can reduce compiler complexity and runtime overhead. In any operating system, when the kernel code is paired with hardware at the physical level, forbidden states appear—a zero tuple of data, which the processor prohibits accessing even programs in the zero protection ring. Only, the processor module can perform active task context switching in protected mode since when shadow copying the data of the executable code, the programmer cannot get direct access to the information. These collisions are resolved by a new approach—marker scanning, which uses generative tables [11].

In addition to coding the address separation of memory protection rings, the OS of different classes implements a strongly typed interface for interfacing with the processor's hardware core and managing the context of binary code execution, taking into account the compilation and assembly profile—the use of system object markers. The command processing pipeline is as follows. After fetching and issuing by any threading device a command to access the memory, the command enters the LSU functional block for executing memory access commands. The executive memory address prepared in the LSU is then transmitted to the MMU, in which the virtual address is translated into a physical address or a global virtual address. Globally, addressable memory provides not only additional programming convenience, which, as experts expect, should affect the productivity of parallel programming by about ten times. An increase in the efficiency of parallel programs is also expected, since two-way interaction models of the "send–receive" type, as a rule, by long messages, are replaced by one-way interactions using short messages. The reality of achieving greater efficiency with such a transition to a new memory model and organization of computations has already been proven in many experiments [12–14].

5 Conclusion

The results of the "Angara" project became the basis for Chinese work on the strategic supercomputer CT-2 (or ST-2, **C**odename—**S**upercomputer "**T**hunderbolt") in 2009 for the global information system of China's military intelligence. The TSMC factory has now produced prototypes of a 12-core mass multi-threaded microprocessor using 45 nm technology, which is a Chinese-modified version of the Russian J7 microprocessor project for the supercomputer "Angara."

The release of the second generation Colossus processor (GC200) was announced. This processor is already manufactured using 7 nm technology; the die area is 823 mm^2; the number of transistors is 59.4 × 109, even more than in GPU ampere. The number of cores in it has been increased to 1472, but the on-chip memory has been increased significantly, three times, to 900 MB. The peak performance of tensor calculations (FP16/FP32) is doubled, up to 250 TF. The real performance due to internal data memory increased by eight times. Significant attention was also paid to the development of a successful computational node in a 1U construct (height 5 cm) with four GC200s connected through a bridge developed by the same company with DDR4 memory up to 450 GB and a bandwidth of 180 TB/s.

Creation of the "fundamentally new" processors has always been an interesting and worthy undertaking, but it has always been accompanied by strong criticism and controversy, which in the end turned out to be extremely useful and improved the solution. As a matter of fact, we hope to initiate such a discussion of the mt-LWP cores architecture.

References

1. Molyakov AS (2020) Based on reconfiguring the supercomputers runtime environment new security methods. Adv Sci Technol Eng Syst J 5(3):291–298
2. Molyakov AS (2020) Main scientific and technological problems in the field of architectural solutions for supercomputers. Comput Inf Sci 13(3). https://doi.org/10.5539/cis.v13n3p89
3. Semenov AS (2010) Development and research of the architecture of globally addressable memory of a multithread-streaming supercomputer. Dissertation for the degree of candidate of technical sciences. Specialty 05.13.15—computing machines, complexes and computer networks. Moscow, p 224

4. Molyakov AS (2019) China net: military and special supercomputer centers. J Electric Electron Eng 7(4):95–100. https://doi.org/10.11648/j.jeee.20190704.12
5. Molyakov AS (2019) Age of great Chinese dragon: supercomputer centers and high performance computing. J Electric Electron Eng 7(4):87–94. https://doi.org/10.11648/j.jeee.20190704.11
6. Adamov A et al (2019) Main problem directions in the field of domestic element base of supercomputers. Cybersecurity Issues 4:2–12. https://doi.org/10.21681/2311-3456-2019-4-02-12
7. Adamov AA, Pavlukhin PV, Bikonov DV, Eisymont AL, Eisymont LK (2019) Prospective general purpose and specialized accelerator processors alternative to modern GPGPU. Cybersecurity Issues 4:13–21. https://doi.org/10.21681/2311-3456-2019-4-13-21
8. Molyakov AS (2019) New multilevel architecture of secured supercomputers. Curr Trends Comput Sci Appl 1(3). https://doi.org/10.32474/CTCSA.2019.01.000112
9. Molyakov AS (2019) Supercomputer and new generation operating systems. Information security: yesterday, today, tomorrow. International scientific and practical conference: collection of articles of the Russian State Humanitarian University. Moscow, pp 196–200
10. Molyakov AS (2016) A prototype computer with non-von neumann architecture based on strategic domestic J7 microprocessor. Autom Control Comput Sci 50(8):682–686
11. Molyakov AS (2016) Token scanning as a new scientific approach in the creation of protected systems: a new generation OS MICROTEK. Autom Control Comput Sci 50(8):687–692
12. Gorbunov V, Eisymont L (2010) Exascale barrier: problems and solutions. Open Systems 6:12–15
13. Eisymont L (2010) DARPA UHPC—the road to exaflops Open Systems, 12. http://www.osp.ru/
14. Mitrofanov V, Slutskin A, Eisymont L (2008) Supercomputer technology for strategic missions. Electronics: NTB 7:66–79
15. Molyakov AS (2021) Specialized hybrid chinese microprocessors for solving important problems of fundamental medicine and national defense. Biomed J Sci Tech Res 34(4):26876–26881. https://doi.org/10.26717/BJSTR.2021.34.005573

Systematics Review on Detecting Cyberattack Threat by Social Network Analysis and Machine Learning

Rizal Tjut Adek, Bustami Bustami, and Munirul Ula

Abstract This literature review gives an up-to-date overview of studies aimed at analyzing the information contained in social media messages, which reflect malicious activity that threatens cyberspace. This work presented studies aimed at detecting and predicting cyberattacks with the intent of altering, controlling, manipulating, damaging, or affecting victims' digital services, computing equipment, and communications equipment of the victims. The method used in this systematic literature review is based on the model proposed by Petersen et al. The conclusion from the studies showed that the use of machine learning algorithms, deep learning, and natural language processing tools contributes to better detection of threats in social media. For future research, it is necessary to continue the implementation of the most recent tools of machine learning and deep learning and natural language processing, to improve the effectiveness of the results. The findings of this systematic review will enable the researcher to develop methodologies and mechanisms that could help detect and prevent future cyberattacks.

Keywords Systematics literature review · Cyberattack detection · Social media analysis · Twitter posting analysis

1 Introduction

The power of dissemination of information that social networks have, mainly to reach many places, is due to the impulse that the tools derived from information technology (IT) have given it. But although, when technology evolves at very rapid steps to provide more facilities and comforts, in the same way, the risks and threats grow with it [1, 2].

R. T. Adek · B. Bustami
Department of Informatics, Universitas Malikussaleh Aceh, Aceh, Indonesia

M. Ula (✉)
Department of Information System, Universitas Malikussaleh, Aceh, Indonesia
e-mail: munirulula@unimal.ac.id

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_50

This article shows an up-to-date overview of those investigations aimed at the analysis of the information contained in social media messages, having the common objective of detecting the events and/or acts that reflect malicious behavior that threatens cyberspace. The results obtained in each of the investigations allowed their authors to create methodologies and mechanisms that helped detect and prevent the risk of future cyberattacks.

Such investigations used an analytical approach similar to those used in other areas, such as market acceptance of a new product [3] monitoring of political events [4], health [5], economic [6], and events. They precisely make use of the information contained in social network messages. However, the following works are focused on cybersecurity events, such as the detection of different types of cyberattacks [7], the prediction of events related to the execution of a cyberattack [8], and even the possibilities of exploiting a software flaw to execute an attack [9].

It should be noted that most of these studies would not have been achieved without a methodology based on the use of tools from the natural language processing area and supported in some cases by the use of machine learning algorithms or deep learning.

1.1 Social Media and Cybersecurity Events

Social networks have become a great mass medium for the dissemination of information, and today they have reached places where humanity could hardly have imagined exploring. Various topics such as politics, entertainment, technology, and many others are discussed in them. All this diversity of topics has allowed the development of several works dedicated to the analysis of information generated by the users themselves, having these members participate in a way similar to that of social event sensors. The quantity and quality of the information in social networks are heavily reliant on the interaction between its members [10].

Many studies are based on the extraction of information from social networks about a specific event; for example, the analysis of the market impact of a new product [3], the monitoring of a disease within a community [11], the monitoring of preferences during political elections [4], and various others. As a result, among all of these works, there are some whose focus is on the discovery of information from the cybersecurity field, and then they use all of this information to create tools or mechanisms of prevention about futures. events and risks that threaten cyberspace.

Concern about the risk of being victims of different types of cyberattacks, and that these can cause damage to infrastructures and computing services, businesses, companies, and even government institutions, has generated great interest on the part of many researchers to be able to anticipate these attacks. The importance of analyzing the communities and information contained in social networks has been highlighted by studies such as Saidi [6]. It can extract information and provide an in-depth look at the operations of clandestine cyber-terrorist groups using the modeling and semantic analysis.

2 Research Method

The research methodology for systematic literature review mapping used in this study is based on the model proposed by Petersen et al. [12] as shown in Fig. 1. The research questions aim to be answered in this study as follows:

- What are the events related to cyberattacks detected in social media networks?
- What are the main cyberattacks distributed on social media networks?
- What information in social networks use for the detection of exploits that could represent a future cyberattack?

The final result of this methodology is the generation of a systematic map about the study topic, which is illustrated, showing the frequencies of publications of each category.

2.1 Search Protocol

In this systematic mapping phase, the search protocol of the research is guided and organized. The essential steps of the process are defined, such as research questions, document screening, abstraction keywords, and data extraction and mapping [12].

Population: research articles related to the area of information security and social media analysis.

- Object: cyberattack.
- Control: social media.
- Results: The analysis of social networks and cybersecurity events and detecting cyberattacks using the information published on social networks.

Two major databases chosen are Google Scholar and the Institute of Electrical and Electronics Engineers (IEEE) Xplore.

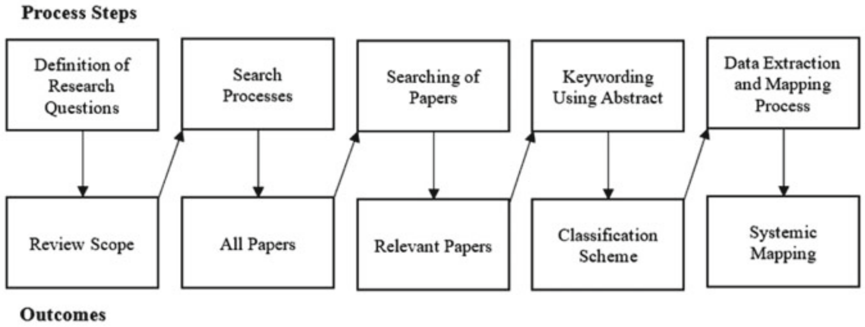


Fig. 1 Systematic mapping study process

2.2 Languages and Filters in Data Sources

The filters determined for the search cover only studies in Computer Science written in English. The terms and synonyms are presented, using the "OR" operator to group the terms and synonyms, and the "AND" operator to select the terms of the question structure: population, object, control, and results. However, the selected databases were Google Scholars because it covers more results than other exclusive databases. The keywords used as follows: ("cyberattack" OR "cybersecurity" OR "hacking" OR "Penetration" OR "intrusion") AND ("social media" OR "Twitter" OR "Facebook" OR "Instagram") AND ("Machine Learning" OR "Deep Learning").

2.3 Data Collection Process

The process is divided into four stages: search in the databases, elimination of redundancies, final selection, and quality assessment. From the search strings generated based on terms and synonyms, a total of 457 articles is returned. After tabulating the articles, the redundancies are eliminated. Altogether, 132 redundancies were found. The title and abstract of the articles are read to select articles related to this study. In all, 21 studies were selected.

3 Result and Analysis

3.1 Detection of Cyberattacks in Social Networks

It is crucial to highlight that the use of the social network to detect cyberattacks cannot be compared to the tools and mechanisms commonly used in the field of cybersecurity, such as antivirus, firewalls, Intrusion Detection Systems, and Intrusion Prevention Systems.

The following works aim to discover threats that may exist in cyberspace, but in an alternative way. Therefore, these are not to be considered as tools to mitigate the different types of cyberattacks. Rather, they only fulfill the function of warning or alerting the discovery of various forms of this type of threat.

This review of the literature reveals four different approaches to detecting cyberattacks: detection of events related to cyberattacks, detection of types of cyberattacks, interest in software vulnerabilities to carry out a cyberattack, and finally cyberattacks on social media. The following subsections show relevant works that are part of this state-of-the-art review.

3.2 Detection of Events Related to Cyberattacks

This section primarily focused on studies related to the prediction and extraction of possible events related to a type of cyberattacks, such as account hijacking and distributed service denial. Table 1 shows a comparison of the results obtained by the research articles in this category. Here it is observed that the most recent algorithms, in machine learning and deep learning, have contributed to the improvement of the results, according to the accuracy in each of the studies. In the same way, it can be seen that the more specific the cyberattack is to detect, the accuracy tends to increase its value.

Ritter [15] demonstrated that a large number of events related to cybersecurity failures are mentioned on Twitter, managing to create an extractor of these events through a semi-supervised method applied to the flow of publications in this social network. While Khandpur [16] developed a method that could dynamically extract those events related to cyberattacks reported and discussed on Twitter, detecting a range of three different types of threats.

Other studies by Hernandez [13, 18] suggest that the response of groups involved in Hacktivism can be predicted when their sentiment is very negative toward a user. Both m All of them gather a corpus of tweets, employ sentiment analysis, and finally use different statistical tools in each job to predict the possible occurrence of the cyberattack.

But not only Twitter has proven to be a recurring social network for obtaining information. Messages from other social networks coming from Hacker forums that reside on the Dark Web have also been analyzed. Such is the work of Goyal [14], where he used deep learning tools (deep neural networks) and time series to predict cyberattacks with information from various Hacker forums.

Deliu [17] concluded with a comparative analysis between Support Vector Machines (or SVM) and Convolutional Neural Networks (or CNN) for the detection ´of these events within forums similar to the previous ones. Finding significantly similar results between both learning tools.

Table 1 Comparison of results between researches focused on the detection of events related to cyberattacks

Research	Objective	Algorithms	Accuracy
Hernandez [13]	Cybersecurity events	Linear regression	0.442
Goyal [14]	Malware, malicious email, Malicious URL	Deep neural networks	0.653
Ritter [15]	DDoS, Hijacking, data	SVM leak + L2 regularization	0.676
Khandpur [16]	DDoS, Hijacking	Kernel Convolution Leak	0.71
Deliu [17]	Malware, Spam, DDoS	CNN, SVM	0.976

3.3 Types of Cyberattacks

The studies presented at this section are aimed at detecting and classifying different forms of cyberattacks on social networks that can trick the user to interact with the content in the messages. As the example such as accessing sites with malware through a URL, social engineering, Spam, malicious content. In such a way that these threats aim to affect and destabilize the system or resource that belongs to the user. Table 2 shows a comparison of the results obtained in each of the previous works. As can be seen, the accuracy tends to rise when the cyberattacks to be detected are specific to one type. On the other hand, this measure increased when the algorithms were supported by tools from the area of natural language processing, as demonstrated in the work of Liao [19]. But it is still pending, to carry out investigations that consider other types of threats such as detection of different types of social engineering attacks, detection of accounts dedicated to the dissemination of these threats, among others.

In Liao [19] they present a framework called iACE whose function is to extract Indicators of Compromise (IoC) [15]) from unstructured texts. The IoC concept is defined as a description of some malicious activity or artifact that is relevant to a cybersecurity incident, and that can be identified through the analysis of its behavior patterns. Based on the above, the author proposes the use of natural language processing techniques (NER/ER) to collect information from public sources such as blogs, articles, and other written media. of public access, and create a series of terms that allow defining unique characteristics of different cyberattacks.

A work dedicated to detecting Phishing was conducted by Wooi [20], where they developed a real-time security alert mechanism that is activated when these types of threats are found in Twitter messages. This research used a classification model derived from machine learning "Random Forest."

Shu [22] used a logistic regression model to predict the behavior of a cyberattack, in the face of threats such as malicious email, malicious URLs, and malware distribution. Previously, they applied sentiment analysis techniques to the flow of Twitter messages to determine the probability of encountering a cyberattack.

Table 2 Comparison of results between researches focused on the detection of cyberattacks in Twitter massage

Research	Objective	Algorithms	Accuracy
Liao [19]	Indicators of compromise NER/ER	SVM	0.95
Wooi [20]	Phishing	Random Forest	0.95
Madissety [2]	Spam	CNN	0.893
Grisham [21]	Malware distribution	RNN	0.87
Shu [22]	Malware, malicious URL, Malicious email	Logistic Regression and PCA	0.644

Madisetty [2] stated a neural network ensemble-based approach to spam detection on Twitter. The model used, at the tweet level, user content characteristics and n-grams. Later, different CNN architectures were added to a neural network, so that they could finally get spam detection. Obtaining a measure F of 0.894. Likewise, investigations have been carried out to identify information that is related to different types of cyberattacks, taking as a source the discussion forums and blogs that reside on the Dark web.

In Grisham [21] they created a method to identify messages that contain information or distribution characteristics of malware applications, and that exposes users who are spreading these threats. In their research, they make use of Recurrent Neural Network architectures (or RNN for its acronym in English) and analysis of the connections between users using graphs. Their results show that sparse files are often in.zip format, and targeted at Android applications. Demonstrating that the majority of users responsible for disseminating this content are those who have some administrative position in this type of forum.

3.4 Interest in Vulnerabilities for the Use of Exploits

Exploits [23] are a type of malware, the malicious programs that contain executable code or data that take advantage of vulnerabilities in software installed on a local or remote computer. These have drawn the attention of malicious users to compromise, extract information and even take control of the attacked computers. Said security flaws in the computing and communications infrastructure software make the assets of the users become victims of these cyberattacks.

There are a couple of concepts for these types of cyberattacks that are mentioned throughout this subsection. The first is a Proof-of-Concept exploit, which is developed as part of a process to expose and report a vulnerability in software, to demonstrate the existence of this security flaw. in the code of the same.

The second concept is real-world exploit [9], these exploits are used to generate cyberattacks on computer equipment, networks, and communication infrastructures of the victims, taking advantage of security flaws in equipment software to achieve an act that is harmful to the user.

The difference between PoC and real-world exploits is that the PoC is not intended to cause damage, but rather they are used to alert the vendor of their software security flaw. However, in the real world, it causes damage and is often developed from the information of the PoC exploits.

The studies in Table 3 are focused on identifying information in social networks to detect the exploits that could represent a future cyberattack. Table 3 shows a comparison of the results obtained by previous studies. As can be seen, the machine learning algorithm, Random Forest shows the best accuracy. Although Mittal [24] did not present a value for this measure, and only reported the number of messages correctly detected within a corpus of tweets. In this work, it is argued that his results improved as he implemented natural language processing tools.

Table 3 Comparison of results between investigations focused on the interest in vulnerabilities for use in exploits

Research	Objective	Algorithms	Accuracy
Sabottke [25]	PoC exploits, real-world exploits	SVM	0.45
Chen [23]	PoC exploits, real-world exploits	FEEU, FRET	0.514
Almukaynizi [9]	Vulnerabilities discussed	Random Forest	0.67
Mittal [24]	Vulnerabilities discussed	NER, SWRL	–

In Sabottke [25] they created a technique that allows detecting the existence of possible real-world exploits, based on information available on the social network Twitter. The number of characteristics obtained to apply in an machine learning model (Support Vector Machine) was 38. Among these characteristics are the text and statistics of the tweets, a marker called Common Vulnerability Score System, and information from a vulnerability database NVD (National Vulnerability Database).

In Mittal [24] they created a framework called CyberTwitter, which has the function of analyzing information contained in Twitter messages, finding the vulnerabilities that represent a threat, and being able to alert the user of the threats. To represent the cybersecurity concepts ontologies, CyberTwitter employs natural language processing techniques such as NER and RDF sentence handling. It creates an alert system with the use of SWRL rules (Semantic Web Rule Language).

On the other hand, Chen [23] developed a method to analyze information from Twitter messages and to be able to predict when the vulnerabilities will be used in a cyberattack of the real-world exploit or PoC type. He used a graph-based analysis called CVE-Author-Tweet, to discover the set of characteristics to use in his prediction model. In the end, he proposes two models, one for the classification called FEEU, with an average accuracy of 0.514. And the other for the regression, called FRET, the latter being the one that indicates when the exploit will be executed. Based on your results, you can predict the use of exploits since the vulnerability appeared, 37.5 days earlier for the PoC exploit, and 11.9 days earlier for real-world exploits.

A study that considered information from social networks and forums of the Deep/Dark web was carried out by Almukaynizi [9], where they addressed the probability of using an exploit as a binary classification problem; positive if it tends to be used or negative otherwise. They used a Random Forest classification model, achieving average results of 0.57 for precision, 0.93 for recall, and 0.67 for an accuracy.

3.5 Cyberattacks on Social Media

This section refers to works whose objective is the detection of cyberattacks directed from one account to another within the same social network. For example, identity

Table 4 Result of the investigation focused on cyberattacks between accounts of the same social network

Research	Objective	Algorithms	Accuracy
Al-Qurishi [1]	Sybil	Deep regression model	0.86

theft or falsification, increase or loss of reputation, account control for use in botnet-type attacks, among other new forms of cyberattacks adapted to these communication sites.

In Al-Qurishi [1] they created a system for predicting the execution of a Sybil-type cyberattack, analyzing information contained in Twitter. In this threat, the attacker can create multiple false accounts or even install malware on the victim's computer, so that later that computer makes likes or reviews, and the victim user is not aware of this. The objective of the attack is to increase or reduce the reputation of a user account. This study employs three steps; data collection modules, a feature extraction mechanism, and a deep regression model using TensorFlow. The result achieved is 86%, as shown in Table 4.

Only one job has been identified related to the detection of a cyberattack, which objective is to control or affect the account of a specific user from another account of the same social network.

4 Conclusion

There are various threats in social media networks such as identity theft, spreading false news, social engineering messages, and many other frauds.

The goal of this research is to conduct a state-of-the-art literature review on the detection and prediction of various types of cyberattacks using social media posting.

Our study concludes that the use of machine learning, deep learning, and natural language processing tools contribute to the better detection of many types of threats in social media posting messages.

From this review, there are two prospects for future research. The first prospect is to improve the accuracy value (F1) in predicting the vulnerabilities to exploits. The second prospect is research related to the detection of cyberattacks on the same social network. However, in future research methodology, it is necessary to implement the most recent algorithms of machine learning, deep learning, and natural language processing tool, to improve the effectiveness of results.

References

1. Hariguna T, Rahardja U, Aini Q, Nurfaizah (2019) Effect of social media activities to determinants public participate intention of e-government. In Procedia Comput Sci 161:233–241. https://doi.org/10.1016/j.procs.2019.11.119
2. Madisetty S, Desarkar MS (2018) A neural network-based ensemble approach for spam detection in twitter. IEEE Trans Comput Soc Syst 5(4):973–984. https://doi.org/10.1109/TCSS.2018.2878852
3. Sukmana HT, Hariguna T, Lutfiani N, Rahardja U (2019) "Exploring the moderating effect of technology readiness of user intention in the context of mobile payment service." Int J Adv Trends Comput Sci Eng 8(1.5 Specia):249–257. https://doi.org/10.30534/ijatcse/2019/4481.52019
4. Younus A, Qureshi MA, Saeed M, Touheed N, O'Riordan C, Pasi G (2014) "Election trolling: analyzing sentiment in tweets during Pakistan elections 2013." In WWW 2014 companion—proceedings of the 23rd international conference on world wide web, pp 411–412. https://doi.org/10.1145/2567948.2577352
5. Khan MAH, Iwai M, Sezaki K (2012) "A robust and scalable framework for detecting self-reported illness from twitter." In 2012 IEEE 14th international conference on e-health networking, applications and services, healthcom 2012, pp 303–308. https://doi.org/10.1109/HealthCom.2012.6379425
6. Saidi F, Trabelsi Z, Salah K, Ben Ghezala H (2017) Approaches to analyze cyber terrorist communities: survey and challenges. Comput Secur 66:66–80. https://doi.org/10.1016/j.cose.2016.12.017
7. Ula M, Ula M, Fuadi W (2017)"A method for evaluating information security governance (ISG) components in banking environment." J Phys Conf Ser 812(1). https://doi.org/10.1088/1742-6596/812/1/012031
8. Adek RT, Ula M (2020) "A survey on the accuracy of machine learning techniques for intrusion and anomaly detection on public data sets." In 2020 International conference on data science, artificial intelligence, and business analytics, DATABIA 2020—proceedings, pp 19–27. https://doi.org/10.1109/DATABIA50434.2020.9190436
9. Almukaynizi M, Grimm A, Nunes E, Shakarian J, Shakarian P (2017) "Predicting cyber threats through hacker social networks in darkweb and deepweb forums". https://doi.org/10.1145/3145574.3145590
10. Urolagin S (2017) "Text mining of tweet for sentiment classification and association with stock prices." In 2017 international conference on computer and applications, ICCA 2017, pp 384–388. https://doi.org/10.1109/COMAPP.2017.8079788
11. Sabe MA et al (2016) "Coronary artery disease is a predictor of progression to dialysis in patients with chronic kidney disease, type 2 diabetes mellitus, and anemia: an analysis of the trial to reduce cardiovascular events with aranesp therapy (TREAT)." J Am Heart Assoc 5(4). https://doi.org/10.1161/JAHA.115.002850
12. Petersen K, Feldt R, Mujtaba S, Mattsson M (2008) "Systematic mapping studies in software engineering." In 12th international conference on evaluation and assessment in software engineering, EASE 2008, pp 68–77. https://doi.org/10.14236/ewic/ease2008.8
13. Hernandez-Suarez A et al (2018) Social sentiment sensor in twitter for predicting cyber-attacks using $\ell 1$ regularization. Sensors (Switzerland) 18(5):1380. https://doi.org/10.3390/s18051380
14. Goyal P et al (2018) "Discovering signals from web sources to predict cyberattacks." [Online]. Available: http://arxiv.org/abs/1806.03342
15. Ritter A, Wright E, Casey W, Mitchell T (2015) "Weakly supervised extraction of computer security events from twitter." In WWW 2015—proceedings of the 24th international conference on world wide web, pp 896–905. https://doi.org/10.1145/2736277.2741083
16. Khandpur RP, Ji T, Jan S, Wang G, Lu CT, Ramakrishnan N (2017) "Crowdsourcing cybersecurity: cyber attack detection using social media." In International conference on information and knowledge management, proceedings, vol Part F131841, pp 1049–1057. https://doi.org/10.1145/3132847.3132866

17. Deliu I, Leichter C, Franke K (2017) "Extracting cyber threat intelligence from hacker forums: support vector machines versus convolutional neural networks." In Proceedings—2017 IEEE international conference on big data, big data 2017, vol 2018-January, pp 3648–3656. https://doi.org/10.1109/BigData.2017.8258359
18. Hernandez A et al (2016) "Security attack prediction based on user sentiment analysis of Twitter data." In Proceedings of the IEEE international conference on industrial technology, vol 2016, pp 610–617. https://doi.org/10.1109/ICIT.2016.7474819
19. Liao X, Yuan K, Wang X, Li Z, Xing L, Beyah R (2016) "Acing the IOC game: toward automatic discovery and analysis of open-source cyber threat intelligence." In Proceedings of the ACM conference on computer and communications security, vol 24–28, pp 755–766. https://doi.org/10.1145/2976749.2978315
20. Liew SW, Sani NFM, Abdullah MT, Yaakob R, Sharum MY (2019) An effective security alert mechanism for real-time phishing tweet detection on Twitter. Comput Secur 83:201–207. https://doi.org/10.1016/j.cose.2019.02.004
21. Grisham J, Samtani S, Patton M, Chen H (2017) "Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence." In 2017 IEEE international conference on intelligence and security informatics: security and big data, ISI 2017, pp 13–18. https://doi.org/10.1109/ISI.2017.8004867
22. Shu K, Sliva A, Sampson J, Liu H (2018) "Understanding cyber attack behaviors with sentiment information on social media." In Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), vol 10899 LNCS. Pp 377–388. https://doi.org/10.1007/978-3-319-93372-6_41
23. Chen H, Liu R, Park N, Subrahmanian VS (2019) "Using twitter to predict when vulnerabilities will be exploited." In Proceedings of the ACM SIGKDD international conference on knowledge discovery and data mining, pp 3143–3152. https://doi.org/10.1145/3292500.3330742
24. Mittal S, Das PK, Mulwad V, Joshi A, Finin T (2016) "CyberTwitter: using twitter to generate alerts for cybersecurity threats and vulnerabilities." In Proceedings of the 2016 IEEE/ACM international conference on advances in social networks analysis and mining, ASONAM 2016, pp 860–867. https://doi.org/10.1109/ASONAM.2016.7752338
25. Sabottke C, Suciu O, Dumitras T (2015) "Vulnerability disclosure in the age of social media: exploiting twitter for predicting real-world exploits." In Proceedings of the 24th USENIX security symposium, pp 1041–1056

Adaptive Multi-attention for Image Sentence Generator Using C-LSTM

K. A. Vidhya, S. Krishnakumar, and B. Cynddia

Abstract Capturing image feature and multi-object region of an image and transferring it into a Natural Language Sentence is a research issue needs to be addressed with natural language processing. Technically, the attention mechanism will force every word representation to an corresponding image region, however at times it do neglect certain words like 'the' in the description text, as it misleads the text interpretation. The captioning of an image involves not only detecting the features from various images, but also decoding the collaborations between the items into significant image text. The focus of the suggested work, predicts the image sentence in a more detailed way for every region/frame of an image. To overcome, an image feature extraction is carried out using CNN and LSTM for the image text generation with the help of adaptive attention mechanism, which will be add in the layer of LSTM to predict better image sentence is constructed. The above mentioned deep network methods have been analyzed using two output combination. Experiments have been implemented using Flickr8k dataset. The implementation analysis illustrates that adaptive attention performs significantly better than without adaptive attention of image sentence model and generates more meaningful captions compared to any of the individual models used. From the results on test images, the suggested network gives the accuracy, bleu score with and without using adaptive attention in the LSTM of 81.53, 61.94 and 73.53, 57.94%.

Keywords Image processing · Deep learning · CNN · LSTM · Bleu score

1 Introduction

Artificial Intelligence (AI) is an area of research which is widely used to address the day to day challenging real world problems [1]. Deep learning yields high precision

K. A. Vidhya (✉) · S. Krishnakumar
Department of IST, Anna University, Chennai, India
e-mail: avidhya06@gmail.com

B. Cynddia
Department of CSE, Shiv Nadar University, Chennai, India

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_51

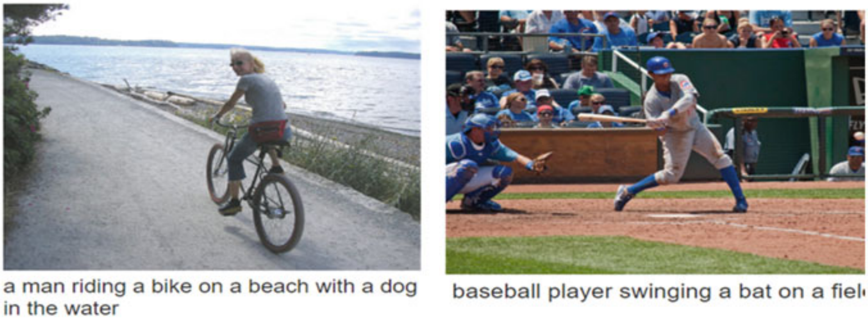
compared to machine learning techniques in Image Processing domain. The task of creating a logical sentence from a picture is tedious process, however it aids in helping those with visually impaired to have a better insight of the images with text representation [2]. The captioning method of the image is complex process when compared to the image classification task, which was the main focus of the research community over half a decade. The summarization of the image should include the interconnection between the objects in the picture. For another improvement to visual comprehension of the image, the above semantic information should be interpreted in a regular language such as English, which requires an appropriate language model.

The DenseNet model used for the LSTM network works in much the same way as for machine translators. The images are converted into a size of 224 * 224 and fed as input layer to CNN. Flickr8k database is used to train the CNN model. A dictionary is created using the caption tokens generated by the training set which forms a baseline text for various image frames. The captions generated are compared to captions given by a human expert on a BLEU score.

Though most of the deep learning approaches have made huge strides in image interpretation activities [3], yet there are many issues to be addressed in the literature. The existing image captioning techniques focus on using an RNN and CNN, bypassing certain influential factors which contributes to the overall sentence generation [4]. The attention-grabbing technique maps each descriptive word to an image region with randomly assigned weights, regardless of the fact certain caption like stop words in the text do not depict the quality structures of the image region [5–7].

Two stage adaptive attention is proposed, where an image caption model with C-Bi-LSTM network is constructed to process the images frames and the text features are mined using glove [8]. In particular, for the first time, the DenseNet system is used to elucidate global features including little nuances of the images. Likewise, each image of five different caption is converted into vector form by using tokenization and fused both image and word vector into one 1-D [9]. After that the dynamic focus approach can automatically determine when it relies on visual cues and relies solely on the language prototype model. Lastly, the elucidated features are given as input to the C-LSTM generates sentence, as decoder output. When compared to past algorithms, the suggested model presents a flexible attention span to show improvement and eradicate the problem of forced communication between expressive words or image.

NLP has a major contribution to artificial intelligence that includes with human–machine interaction in natural language [10]. The core objective of the NLP is to understand the natural languages that system or machine generates. Wide range of research has been approved with respect to text caption generation which aids in field of application and interaction to a number of other traditional artificial intelligence areas. Natural language sentence generation tasks are naturally overwhelmed with defectiveness, such as exclusions, inconsistencies and mistakes. These have created challenges in categorizing from instructions. A machine should be able of understanding natural language instructions in an unambiguous manner. To overcome this above need, this work aims toward categorizing the natural language instructions. Here the focus is on English language text, particularly with instructions.



a man riding a bike on a beach with a dog in the water

baseball player swinging a bat on a fiel

Fig. 1 Image sentence generation with and without attention

In the upcoming sections, we discuss briefly about the model used. The CNN encoder and the LSTM decoder are discussed in detail. The code for both modules are explained briefly. We used the BLEU score metric to compare the accuracy of the model proposed with the ones already present. At the end, we report a few examples tested on the model. Figure 1 shows Image captioning with adaptive attention, it gives more detailed portrayal of the image and also it shows Image Captioning without adaptive Attention which predicts normal portrayal of the image.

The flow of the paper is indicated as follows. Section 2 describes literature survey done in the arena of image caption prediction. Section 4 provides the system design of this work. Section 5 shows implementation of the offered modules and the results of the suggested modules. Section 6 at last summarizes the Conclusion and Future Work meticulously.

2 Literature Survey

Wang et al. [11] proposed a challenging issue, creating photo captions automatically on its own and has attracted increasing attention in the study of indigenous languages and in computer-based communities. In this paper, the authors suggested a deep end-to-end learning method for producing photo captions. They used a picture feature details at a set moment each minute and produce an equivalent caption using a semantic attention prototype. The framework mitigates us to introduce frames as repeating structure which is also a focus module, obtained by computing the similarities between an image element the sequence along with the meaning of a word. The model is intended to transmit information the presentation found in the English section went to the Chinese section to attain a different expression photo caption. The planned model reports 3.9% improvement over existing modern captions for image captions in a different language Flickr8k CN database in CIDER matrix.

Sharma et al. [12] proposed this model enables a person to enter image and extract the same description. The paper uses deep learning as well natural language processing (NLP) to generate captions. Moreover, picture captions generation is a significant task as it agrees us to use the equipment of captioning function for any image. This works enables us to easily edit files without listening to caption function. This paper aids in help for visually impaired people or suffer from short vision. Therefore, instead of looking at image problem can easily read the generated captions with this model in a larger format. It can also be used to donate real-time video description for later use of video.

Mohan et al. [13] proposed Image Caption Generator works by writing captions of an image. Moreover, semantic connotation of an image is apprehended and converted into natural language text. The process of making the system to understand and interpret an image is a tedious task that includes image processing and text analytics. The machine. Mohan et al. [13] proposed Image Caption Generator works by writing captions. The image is depicted as an innate language based on the meaning of the image. The photography method interacts with both images and its management. The machine must monitor and build interactions between objects and living beings. In this paper one can discover, identify and make footnotes using in-depth reading. The Regional Object Detector (ROD) is used to perceive and create subtitles. The paper is based on in-depth education to improve the development of current photo captioning system. Flickr 8 k database is used during tests to indicate the route via python.

Bajpayee et al. [14] resolved the file for problem finding image captions. The system is trained about the interaction between text and pictures from the given labeled images. Its uplifting automated method by incorporation of CNN and RNN. The encoder is trained to comprehend the available aspects in the included illustration used for in the final step. The model tries to produce captions for all aspects. Treatment speech as a major area of the label, the model gives predictions of the various regions of the image and merge them.

Sarfi et al. [15] proposed the inclusion of photo captions is a significant short-term tasks in machine learning. Application encoder decoder the structures are also used. With visual imagery, with encoder, most of these networks use the final layer of network specification is designed for specific computer viewing functions. There are several down to that first of all, these are special models to find some objects from the image. So, when the deeper into the file network, network focuses on these things, it becomes almost do not see the whole picture. These are encoder dots sometimes this is where the next word in the title ends. In addition, most words in the captions are not included in the target categories of these functions, similar to 'snow'. There is an aim to reduce the blind spots of the last layer of the coding decision, and suggestions are specified to other layers of encoding specification. Doing so gives us different aspects of the image while it is not ignoring almost any part of the image is why we go there in everything in the illustration.

Parmar et al. [16] proposed defining the content of an image without a person intervention is a difficult task. Computer and environmental perspective language processing is commonly used to overcome this problem. It requires a two-way approach, to understand image content using computer view, modify the file understands appropriate sentences. Conversion neural network is a powerful and widely used image feature procedure for extracting object detection and image classification. Gated Recurrent Unit (GRU) is often used for efficiency sentence generation. An integrated CNN and GRU model were available proposed to achieve accurate photo captions. And a suggestion model, tests are executed on various data sets as well compare results with existing work. BLEU test metrics used to ration results; proposed the ideal results in BLEU-4 points (increasing significantly) in Database for MS COCO 2017 as 53.5.

3 Problem Statement

In the literature the most important factor of description is feature information extraction, and another aspect is how to completely use characteristic information, its lead accuracy was low and also meaningless evidence of the image. Hence, a CNN-based multi-label for the image region and LSTM with adaptive attention mechanism via visual sentinel method has been planned. The aim of this project is to generator detailed image description of the picture of each region present in it and to get the most accurate information.

- To generate the text and images with an acceptable semantic order.
- To predict correct semantic order and then organize the image depiction by first foreseeing semantic concepts.
- To improve Image description more in detail by using adaptive attention mechanism in C-LSTM.

The outcome of the proposed work is to generate image sentence in the detailed way by taking into description of every region present in image using adaptive attention mechanism via visual sentinel method applied in decipherer aspect of the LSTM layer. The pictorial caption prediction has been implemented in convolutional neural network (Dense Net) architecture, converting word to vector using tokenization and giving input to the long short-term memory phase. Precision of a subtitle of an illustration prediction for training images and test images will be identified. Finally, output will be generated image sentence with help of adaptive attention and without adaptive attention. To resolve the problem of single-feature extraction output and the attention-grabbing method that compels each caption to be found, this paper puts forward a captioning image with a complex network with adaptive attention, which enhances precision and elasticity of subtitles for images.

4 Proposed Work

Figure 2 depicts the system architecture of subtitles for images prediction is to describe the detailed material of the present region in the images using CNN and LSTM architecture with the help of adaptive attention. The steps in the design process

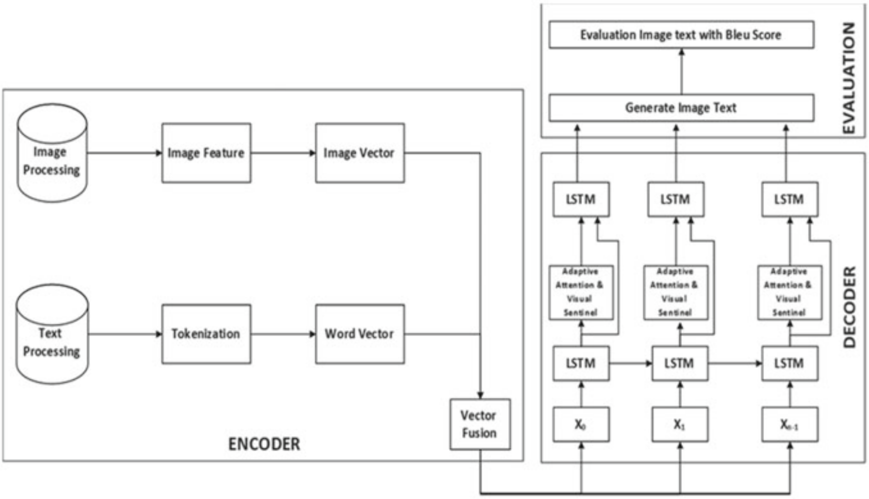


Fig. 2 System architecture of image captioning

includes preprocessing, convolutional neural network, tokenization of the text dataset and final stage is to foresee the image caption in test image dataset. Image caption prediction is implemented in CNN and LSTM neural network. Finally, the accuracy of training and test images are calculated.

Image sentence generator is implemented using google Colaboratory platform, python language and python packages (OpenCV, TensorFlow, torch, Keras and, etc.). There are many data sets open and available in this project resource regard such as Flickr 8 k (containing 8000 images) MS COCO (containing 180,000 images), Flicker-30 K (containing 30,000 images) and so on in our first use of the Flickr 8 k database. This data comprises 8000 images each with 5 captions divided as 6000 images for training sets, 1000 validation sets and another 1000 test set [9]. This database is out of date associated to other data sets and has a partial number of images to fit a wide range of applications. However, it difficult for normal CNN [17–19] networks to learn the features since, most of multi-label object to predict and also train more multi-label images. Therefore, there is a need for using pre-trained CNN of DenseNet121 Architecture. Preprocessing consists of resizing the images (224 × 224) and changing into vector of the image and text data also in order to fuse both the image vector and text figures of the production [20].

The starting stage of encoding uses the DenseNet-121 network with Dense Blocks and Transition layers. The first pass of the convolutional layer uses 2000 filters which is got using filter of 7*7 which is then conceded on through the max assembling layer with a window size of $3 * 3$ with pace 2 features.

The output generated will be a feature vector of $56 * 56 * 2000$ is obtained, and the feature vector of $56 * 56 * 2000$ is finally input into Dense Block 1.

There are 4 dense layers with three intermediate layers, an average pooling layer of 7 ∗ 7 is used to output the feature vectors of the image. Firstly DenseNet extract the images features and skip gram model is used to create word vectors. The image features are $v = \{v1, v2, v3,\ldots, vL\}$, $vi \in \Re D$,

Both the image vector and text features are fused together to form $xt = \{vt, st\}$. In the second step, the image aspect C considering weight is found by utilizing an adaptive catered mechanism prototype where the pictorial aspect V and x (fused vector) are prepped. LSTM network needs the key consisting of image aspect C and the text aspect S by which create a detailed description sentence in the third step.

In steps involved in data preprocessing are listed below.

Step 1: Providing image input to the pre-trained DenseNet121 architecture.
Step 2: Resizing the image to 224×224.
Step 3: Getting output as extracted aspect of the multi-label image.
Step 4: Converting into vector *form of the* removed element.
Step 5: Text preprocessing.
Step 6: Tokenizing the text data splitting the sentence into *word by word*
Step 7: After changing into single word converted into vector form
Step 8: Merging the two vectors of the output of image and text.

A major tokenization used would be word tokenization. On the basis of a particular delimiter it breaks the word lines into separate parts. Based on the restrictions, different tokens at the word level are generated. A few examples for pre-trained word embedding would be Word2Vec and Glove. In many languages, text is made up of words separated by whitespace, where each word has a specific meaning. In next section how the sign languages are modified is discussed, the problem of a sign having a more multifarious meaning than a word is also presented. In the time being, how the words are represented in English is given below.

Example:
Raw text: I had a dinner, and it was better.
Tokenized text: [’I’,’had’,’a’,’dinner’, ‘,’, ‘and’,’it’,’was’,’better’, ‘.’].

The first module extracts the image feature by using a pre-trained convolutional neural network model of DenseNet121 architecture to detect the multi-label region present in the images. Keras applications are deep learning models that are made accessible with pre-trained weights. So, these models can be used for predict, feature extraction purposes and fine-tuning process. After extracting features from the images, it will convert into vector of the features by flattening to 1-D. DenseNet model is to describe the detailed information of the dense block and convolution region in the look used to obtain features of the images. DenseNet, this allows to detect each separable object in images, locate their position and size as well relative to the rest of the image. FLICKR8K dataset has many multi region images are preprocessed to 224×224 dimensions which will helps to train normally for the learning the image features.

Vector fused input from the both image and text dataset, it given input to the LSTM for the training the model. After the initial tier passes the output to adaptive attention layer. This adaptive attention tier will modify weight of the region in the image and also text in the sentence will identify remaining small objects and gives detailed description. The research contains two distinct Encoders, where the initial step utilizes DenseNet121, and the next utilizes tokenization. All processes stop during the teaching process and continue during the fine-tweaking stage. DenseNet121.

LSTM is a neural network that uses recurrent technology to obtain the information provided as a lengthy order and also obtain the solution to gradient loss and passed on to neural networks. In standard RNN, all its aspects are reconfigured by time back propagation (BPTT). The slope of the succeeding nodes decreases during the back distribution process, thereby complicating the upgrades for the existing nodes and causing the model performance to not succeed. It can be observed that when the time phase takes too much time, the succeeding nodes are unable to obtain data easily, during the test phase and it is challenging to explain the question of ‘’ extended support ‘’ timeline, and the accuracy of the forecast is incorrect.

The three memory gates in LSTM are,

- Input gate—controls the input information
- Forget gate—enables LSTM to forget unnecessary information
- Output gate—enables to output the information to next cell.

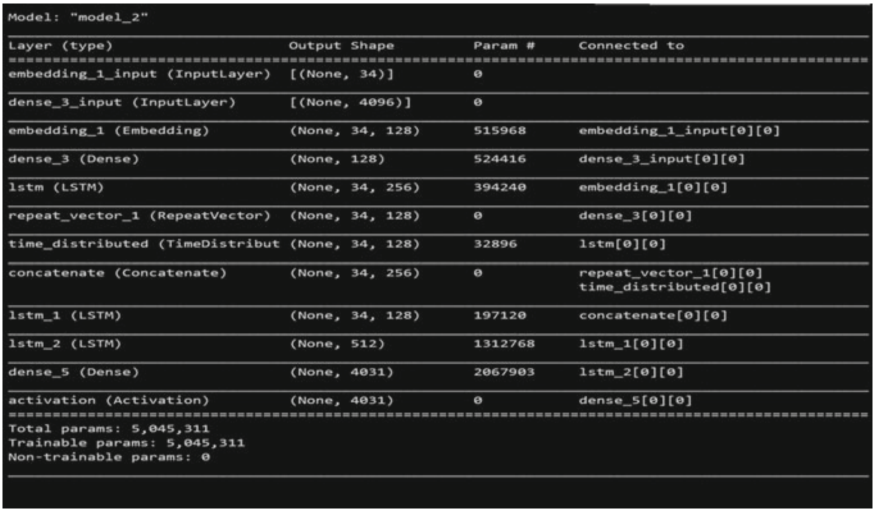
An LSTM cell was created as the answer to the question. Memory cells are inserted using gates and these are used to store common knowledge and gates are used substitute the changes during the restoration of memory cells.

The LSTM acts as a basic communication model which has attention composition for image retrieval. The proposed work replaces the values of vector generated by the fully connected CNN with the DenseNet layer that usually creates a multi-view point on other parts of the images.

The visual sentinel *st* is used to extend the attention model of the upper section to construct a visual sentinel formula created on the LSTM memory unit:

$$\mathbf{g_t} = \theta\left(\omega_{\mathbf{x}}^{\mathbf{x}}\mathbf{t}^{+\omega\mathbf{h}}\mathbf{h_{t-1}}\right) \tag{1}$$

$$\boldsymbol{S_t} = \boldsymbol{g_{t^{\emptyset}}} \tan \boldsymbol{h}\left(\tilde{\boldsymbol{h}}_t\right) \tag{2}$$



```
Model: "model_2"
__________________________________________________________________________________________________
Layer (type)                    Output Shape         Param #     Connected to
==================================================================================================
embedding_1_input (InputLayer)  [(None, 34)]         0
__________________________________________________________________________________________________
dense_3_input (InputLayer)      [(None, 4096)]       0
__________________________________________________________________________________________________
embedding_1 (Embedding)         (None, 34, 128)      515968      embedding_1_input[0][0]
__________________________________________________________________________________________________
dense_3 (Dense)                 (None, 128)          524416      dense_3_input[0][0]
__________________________________________________________________________________________________
lstm (LSTM)                     (None, 34, 256)      394240      embedding_1[0][0]
__________________________________________________________________________________________________
repeat_vector_1 (RepeatVector)  (None, 34, 128)      0           dense_3[0][0]
__________________________________________________________________________________________________
time_distributed (TimeDistribut (None, 34, 128)      32896       lstm[0][0]
__________________________________________________________________________________________________
concatenate (Concatenate)       (None, 34, 256)      0           repeat_vector_1[0][0]
                                                                 time_distributed[0][0]
__________________________________________________________________________________________________
lstm_1 (LSTM)                   (None, 34, 128)      197120      concatenate[0][0]
__________________________________________________________________________________________________
lstm_2 (LSTM)                   (None, 512)          1312768     lstm_1[0][0]
__________________________________________________________________________________________________
dense_5 (Dense)                 (None, 4031)         2067903     lstm_2[0][0]
__________________________________________________________________________________________________
activation (Activation)         (None, 4031)         0           dense_5[0][0]
==================================================================================================
Total params: 5,045,311
Trainable params: 5,045,311
Non-trainable params: 0
__________________________________________________________________________________________________
```

The decoder's reminiscence stores long- and short-term graphical and semantic information. This new component is called the visual sentinel. A deep neural network is prepared by shuffling its aspects (neurons) to enhance its problem-solving skills. The estimated outcome is compared with the actual ground outcome and correct weights are used to eliminate the error using a loss function. The failure event is used to assess the quantity the model should seek to reduce during training. In retrospective models, the commonly used loss function used is a mean square error function while the segment models predict the probability, the most common loss function is cross entropy. This project uses classical cross entropy.

It is a loss function used in multi-class classification functions. It is an optimization function used in the training of the data-segregation model by predicting that data may belong to one category or another. In the proposed work, experiments have been taken out utilizing Flickr8k dataset comprising 8000 images and 5 unique titles for every picture. The bleu score performance system is used to assess the calculations. It shows that adaptive attention is superior than without adaptive attention of image sentence model and also creates more accurate subtitles compared to other models. From the investigational findings on test images, the proposed network gives the accuracy, bleu score with and without using adaptive attention in the LSTM of 81.53, 61.94, 73.53 and 57.94%.

The loss event is used to calculate the quantity the model should seek to reduce during training. In retrospective models, the commonly used loss function used is a mean square error function while the segment models predict the probability, the most common loss function is cross entropy.

It is a loss task used in multi-class classification functions. It is an optimization function used in the preparation of the data-segregation model by predicting that data may belong to one category or another. The function is best for classification problems in multi-class classification problem. It be considered as possibilities over the outcome, the result is standardized such that the additive result is 1. It is also applied finally in a classified type including cross information as loss function (Eq. 3).

$$\boldsymbol{Relu}(\boldsymbol{f}(\boldsymbol{x}) = \max(0, \boldsymbol{x}) \tag{3}$$

$$\sigma\left(\vec{z}\right)_i = \frac{e^{z}i}{\sum_{j=1}^{k} e^{zj}} \tag{4}$$

The problem that continues is how each load should be adjusted to improve the performance of our brand. To find a way to minimize the loss, Adam optimizer is used.

$$\theta^* = \arg\max_{\theta} \sum_{\mathbf{c},\mathbf{s}} \sum_{\mathbf{t}=0}^{\mathbf{N}} \log \mathbf{P}(\mathbf{s}_\mathbf{t}|\mathbf{c}, \theta, \mathbf{s}_0, \mathbf{s}_1 \ldots \mathbf{s}_{\mathbf{t}-1}) \tag{4}$$

The model learns the parameter θ.

Length of sentence is denoted by *n*.

The individual weights are given by $c \in \{c1, c2, \ldots, ct\}$ and overall feature is represented as C. The picture *S* is a sentence that correctly describes the picture.

si is every word vector included in the sentence.

5 Performance Evaluation

The pipeline is still not completely accurate and be studied properly. To rectify that the model is prepared such that it can study with accuracy. Even after the prototype is rectified, a key part of the model still remains uncompleted.

One of the major ways to showcase the caption generator's performance is via line production and accuracy of evaluation and is thus very crucial. Assessment system of measurement BLEU-1, BLEU-2, BLEU-3 and BLEU-4 which can inferred from Figs. 3 and 4 (Bilingual Evaluation Understudy) are the major system of measurement to assess the value of the line creation using natural language managing technique. 4-g BLEU score (BLEU-4) is the first assessment system of measurement used for enhancement.

Figure 5 show the result of the final outcome of this project. Final process in this architecture is to test the newly test images which are not included in training and validation process. Outcome of the result will be image sentence without using adaptive attention and another outcome of the result will be generated image sentence very detail description using adaptive attention using a pictorial sentry method in LSTM. Figure show the test image prediction evaluation. A bleu score is a summary of the prediction output on an Image sentence.

Figure 5 depicts the precision of the system is modeled by BLEU score. BLEU is an algorithmic function named after Bilingual evaluation understudy that is used to

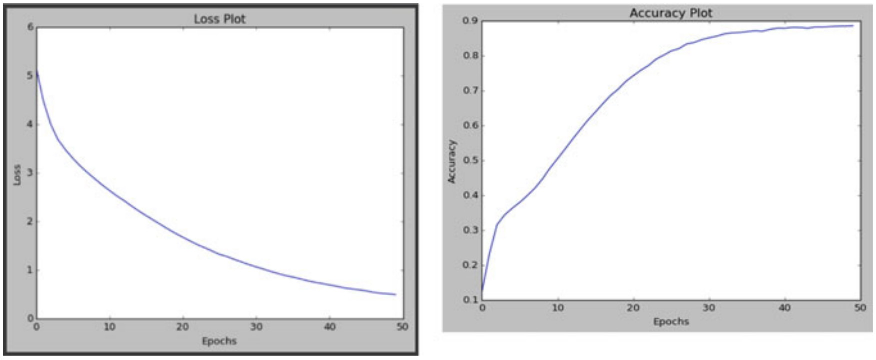
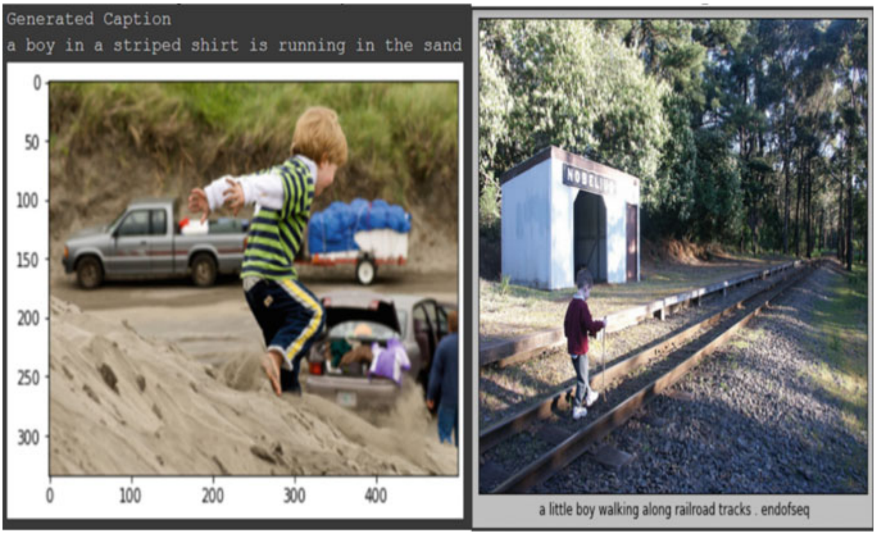


Fig. 3 Accuracy and loss plot with incremental epochs


Generated Caption
a boy in a striped shirt is running in the sand

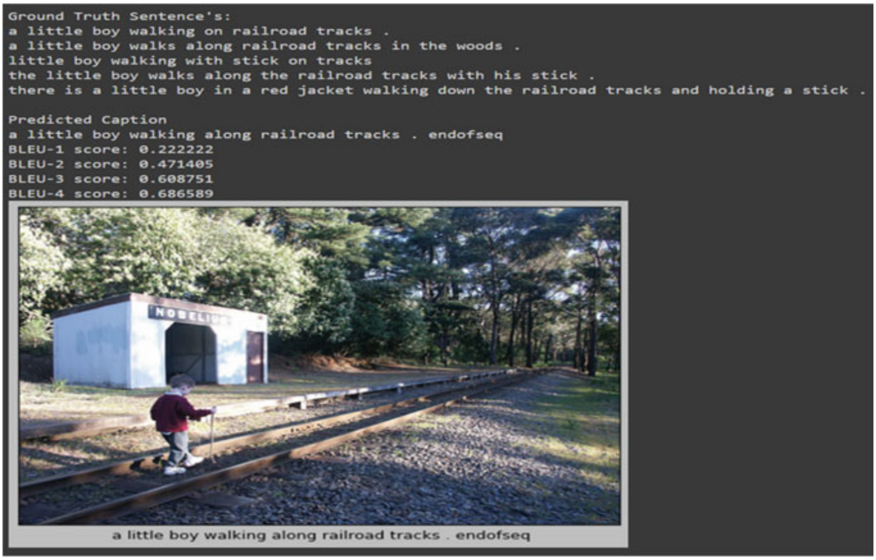
a little boy walking along railroad tracks . endofseq

Fig. 4 Image caption without adaptive attention

evaluate the description of text which has been translated by a machine. This score yields high correlation score when compared to expert score. The range of the bleu score is from 0 to 1 and, whereas 0 is assigned when there is no relation between the sentence generated and the reference sentence. BLEU's evaluation method requires following inputs like:

(i) Numerical translation metric, given and measured by comparison
(ii) A combination of human reference versions.

Table 1 discusses the hyper-parameters used to model the Bi-LSTM for text and visual attention for Image sentence generation. Additionally Table 2 outlines the bleu



```
Ground Truth Sentence's:
a little boy walking on railroad tracks .
a little boy walks along railroad tracks in the woods .
little boy walking with stick on tracks
the little boy walks along the railroad tracks with his stick .
there is a little boy in a red jacket walking down the railroad tracks and holding a stick .

Predicted Caption
a little boy walking along railroad tracks . endofseq
BLEU-1 score: 0.222222
BLEU-2 score: 0.471405
BLEU-3 score: 0.608751
BLEU-4 score: 0.686589
```

a little boy walking along railroad tracks . endofseq

Fig. 5 Image caption without adaptive attention bleu score

Table 1 Modeling hyper-parameters

Sigmoid attention mechanism
Batch size 64
Relu—optimization function
Epoch—150
Embedding-dimension: 300
Hidden-dimension = 0.5
Dropout = 0.5

Table 2 Comparison with existing approaches

	Bleu-1	Bleu-2	Bleu-3	Bleu-4
Wang et al. [21]	68.8	51.3	37.0	26.5
Tang et al. [22]	72.5	55.6	41.7	31.2
Xu et al. [23]—Soft Attention	70.7	49.2	34.4	24.3
Xu et al. [23]—Hard Attention	66.7	43.4	28.8	19.1
Proposed Work—LSTM	68.8	49.8	38.2	22.1
Proposed Work—Bi-LSTM	79.8	68.6	48.8	38.4
Wang et al. [11]	66.8	46.8	32.2	22.1

score comparison rate with the existing systems and proposed work. The bleu score value is lesser when compared to the bi-LSTM. Next section outlines the conclusion and future work.

6 Conclusion and Future Work

In this proposed paper, capturing image captions is a complicated process as it requires both processor's perspective and comprehension of natural language administering. This paper is framed to follow the full outline of the ‘’ encoder decoder ‘’ where as in the encoding phase, DenseNet is cast-off to excerpt complete pictorial aspects; in the suspension phase, a supplementary ‘’ visual sentry ‘’ for enhancing the forced communication between words and image locations using a LSTM supplement. This approach is deemed to be acceptable by the BLEU metric system. Testing principles and managed to enhance the total execution and accuracy. Test image accuracy of 500 images improved. From the experimental results without using adaptive attention, the epoch value for the 80% of training image and 20% for validation process is 100, which gives the accuracy of 87.57%. The optimal dropout value for the dropout layer is 30%. And also, final results with using adaptive attention, the epoch value for the 80% of training image and 20% for validation process is 20, which gives the accuracy of 80.00%. The optimal dropout value for the dropout layer is 30%.

The future scope of this field is enormous as this technology provides a plan to automate machines that can produce results as close as possible to the individual mind. In the upcoming years this work can be extended to increase the accuracy of the scheme to have the same results as humans. Also, the accuracy of the system can be increased by using data sets with a large amount of relevant information that will be available in the future. In the time to come, the method has the capability to prepare and collect outputs not only in general but as a specific domain that will ultimately increase its accuracy and will help to achieve specific field-specific results.

References

1. Arifianto A, Ramadhani KN, Mahadi MRS (2020) “Adaptive attention generation for indonesian image captioning.” In: International conference on information and communication technology (ICICT), pp 1–6
2. Hani A, Kherallah M, Tagougui N (2019) “Image caption generation using a deep architecture.” In International Arab conference on information technology (ACIT), pp 246–251
3. Yao T, Pan Y, Li Y, Qiu Z, Mei T (2017) Boosting image captioning with attributes. In ICCV, 4904–4912
4. Yang Z, Yuan Y, Wu Y, Cohen WW, Salakhutdinov RR (2016) Review networks for caption generation. In NIPS, 2361–2369
5. You Q, Jin H, Wang Z, Fang C, Luo J (2016) Image captioning with semantic attention. In CVPR, 4651–4659

6. Young P, Lai A, Hodosh M, Hockenmaier J (2014) From image descriptions to visual denotations: New similarity metrics for semantic inference over event descriptions
7. Transactions of the Association for Computational Linguistics 2:67–78
8. Song J, Guo Y, Gao L, Li X, Hanjalic A, Shen HT (2018a) From deterministic to generative: multimodal stochastic rnns for video captioning. IEEE Trans Neural Netw Learn Syst 1–12
9. Song J, Zeng P, Gao L, Shen HT (2018b) From pixels to objects: cubic visual attention for visual question answering. In IJCAI, 906–912
10. Zhang M, Yang Y, Zhang H, Ji Y, Shen HT, Chua T-S (2019) More is better: precise and detailed image captioning using online positive recall and missing concepts mining. IEEE Trans Image Process 28(1):32–44
11. Wang B, Wang C, Zhang Q, Su Y, Wang Y, Xu Y (2020) Cross-lingual image caption generation based on visual attention model. Inst Electric Electron Eng 8:104543–104554
12. Song J, Gao L, Guo Z, Liu W, Zhang D, Shen HT (2017) Hierarchical LSTM with adjusted temporal attention for video captioning. In IJCAI, 2737–2743
13. Mohan A, Laxman K, Vigneswaran D, Yuvaraj J, Kumar NK (2019) Detection and recognition of objects in image caption generator system: a deep learning approach. Int Conf Adv Comput Commun Syst (ICACCS) 9:107–109
14. Bajpayee A, Raghuvanshi D, Mittal H, Bhatia Y (2019) Image captioning using google's inception-resnet-v2 and recurrent neural network. Twelfth Int Conf Contemp Comput (IC3) 5:1–6
15. Sarfi A, Ghasemian F, Asadi N, Karimpour Z (2020) Show, attend to everything, and tell: image captioning with more thorough image understanding. Int Conf on Comput Knowl Eng (ICCKE) 8:001–005
16. Parmar B, Jayaswal D, Parikh H, Sawant H, Shah R, Chapaneri S (2020) "Encoder-decoder architecture for image caption generation." In International conference on communication system, computing and it applications (CSCITA), 174–179
17. Pan C, Ding K, Wang L, Xiang S, Xiao X (2019) Deep hierarchical encoder–decoder network for image captioning. Inst Electric Electron Eng 21:2942–2956
18. Al Fatta H, Hartatik, Fajar U (2019) "Captioning image using convolutional neural network (cnn) and long-short term memory (lstm)." Int Seminar Res Inf Technol Intell Syst (ISRITI) 4:263–268
19. Hu H, Tian J, Li L, Liu M, Guan W (2020) Image caption generation with dual attention mechanism. Inf Process Manage 5:587–521
20. Xia Y, Tian F, Wu L, Lin J, Qin T, Yu N, Liu T (2017) Deliberation networks: sequence generation beyond one-pass decoding. In NIPS, 1782–1792
21. Wang A, Chan AB (2018) "CNN+ CNN: convolutional decoders for image captioning", arXiv preprint arXiv:1805.09019
22. Li L, Tang S, Zhang Y, Deng L, Tian Q (2018) GLA: global-local attention for image description. IEEE Trans Multimed 20(3):726–737
23. Xu K, Ba J, Kiros R, Cho K, Courville AC, Salakhutdinov R, Zemel RS, Bengio Y (2015) Show, attend and tell: Neural image caption generation with visual attention. In ICML, 2048–2057
24. Chen C, Wang EK, Wang F, Wu T, Zhang X (2019) Multilayer dense attention model for image caption. Inst Electric Electron Eng 7:66358–66368
25. Vedantam R, Lawrence Zitnick C, Parikh D (2015) Cider: consensus-based image description evaluation. In CVPR, 4566–4575

A Low-Cost Smart Monitoring Device for Demand-Side Response Campaigns

A. Geri, F. M. Gatta, M. Maccioni, J. Dell'Olmo, F. Carere, M. A. Bucarelli, P. Poursoltan, N. Hadifar, and M. Paulucci

Abstract The energy transition requires an increasing penetration of renewable resources, particularly at MV/LV levels. The emerging production scheme is characterized by distributed power plants, imposes a capillary control of production and consumption among the distribution network (DN). The implementation of demand-side response (DSR) campaigns is widely seen as a solution that can increase grid stability, but they require a complex and expensive monitoring infrastructure to select the optimal operating point of the production/consumption systems. This paper suggests a cheap and reliable smart monitoring device based on Raspberry Pi technology. The communication infrastructure adopted in the smart building of ASM S.p.A., the distribution system operator (DSO) of Terni city, shows the feasibility of implementing this prototype on a large scale.

A. Geri · F. M. Gatta · M. Maccioni · J. Dell'Olmo · F. Carere (✉) · M. A. Bucarelli ·
P. Poursoltan · N. Hadifar
Department of Astronautics, Electric and Energy Engineering, Sapienza University of Rome, Rome, Italy
e-mail: federico.carere@uniroma1.it

A. Geri
e-mail: alberto.geri@uniroma1.it

F. M. Gatta
e-mail: fabiomassimo.gatta@uniroma1.it

M. Maccioni
e-mail: marco.maccioni@uniroma1.it

J. Dell'Olmo
e-mail: jacopo.dellolmo@uniroma1.it

M. A. Bucarelli
e-mail: marcoantonio.bucarelli@uniroma1.it

P. Poursoltan
e-mail: parastou.poursoltan@uniroma1.it

M. Paulucci
ASM Terni S.P.A, Terni, Italy
e-mail: marco.paulucci@asmtde.it

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_52

Keywords Distribution network · Smart monitoring · Demand response

1 Introduction

The penetration of distributed generation among the LV/MV grids and the actual challenge of new electricity-based services, like electric mobility, raised the need for a new grid concept, the so-called smart grid (SG), to manage high fluctuations of production and consumption. SGs require a volume of data to be collected that is increasing tremendously [1], and its secure, efficient, and scalable collection has become a challenging task. The metering infrastructure to monitor DG and loads is requested to be capillary widespread.

In this regard, this paper proposes a cheap and reliable device, based on Raspberry Pi and affordable sensors, for the monitoring of an energy district, in order to implement DSR strategies on a large scale. The feasibility of the monitoring infrastructure for a company building demand is tested in the headquarters of ASM S.p.A., the DSOs of Terni province, in the center of Italy.

As expressed in the literature, SGs represent a significant evolution from traditional power grids, as they allow bidirectional flows of energy and communications. For this grid revolution, a necessary step to be overcome is to monitor the network in detail; therefore, the network must be equipped with a large-scale advanced metering infrastructure (AMI), connected to a data center equipped with computational intelligence technologies and a smart control system, in order to allow accurate and real-time network management [2, 3]. The AMI can be assumed as the developed version of traditional automated meter reading (AMR) and automatic meter management (AMM) systems since it involves several enhanced technologies, such as smart meters (SMs), home area networks (HANs), wide area networks (WANs), or neighbored networks [3, 4]. The capillary monitoring infrastructure is exploited in literature to create services for the DSO and the consumers/prosumers, such as to detect sources of energy flexibility on the territory and to implement DSR or other decision-making mechanisms [5, 6]. Some studies focus on the devices' capability to work with a large quantity of electrical/energy measurements and grid status [7–11]. In [12], smart meters are utilized to provide the grid operators more visibility into the health and operation of their assets (e.g., transformers, lines). In [13], the authors present an original data acquisition and transmission system designed and optimized for online temperature monitoring systems in electric power transformers. In [14], a real-time anomaly detection framework is developed by exploiting data collected at the consumers' premises. In this way, the authors present a system able to detect anomalous events and abnormal conditions. A new method to carry out the load flow analysis in MV networks is presented in [15], based on LV load power measurements applied on an innovative backward/forward algorithm for the power flow resolution. The power quality of public electricity networks is evaluated in [16] through a signal analysis framework based on the data acquisition and transmission of the monitoring devices. Many studies highlight the possibility of building up DSR campaigns to exploit the flexibility derived by the customers [13–21]. In [22], the DSR allows the customers, autonomously or in energy communities, to estimate the baseline price in real time. Based on the estimated price signal, the customers schedule their energy consumption using a cost-sharing strategy to minimize their incommodity level. The authors of [23] suggest an energy management system that runs a simple DSR campaign, considering peak and off-peak rates. Most of the existing studies mainly focus on the theoretical design of DSR schemes and do not verify the proposed schemes through implementation, as underlined in [24].

The activities presented in this paper are carried out and partially financed within the European Union's Horizon 2020 research and innovation program under the IoT-NGIN project [25], which investigates how the diffusion of advanced telecommunication technologies, like 5G, combined with the application of advanced tools of artificial intelligence, can produce significant benefits for the energy system.

The paper is structured as follows: Section 2 illustrates the prototype of smart monitoring device and the telecommunication infrastructure; Section 3 presents the case study of this paper; Section 4 shows the measurement tests in ASM district, and finally, Section 5 concludes the paper.

2 Smart Monitoring Device Components

The smart monitoring device presented within this paper is composed of two Raspberry Pi: a Raspberry Pi 3 model B + and a Raspberry Pi 4. The proposed system monitors four variables: secondary substation temperature, secondary substation humidity, RMS values of voltage and current.

The measurement data are transferred to Raspberry Pi 3 to be stored in and communicated via socket connection provided by a network router (Table 1).

The Raspberry Pi is a single-board computer that runs the Linux operating system and can be used directly in electronics projects due to GPIO pins on the board [26]. The card also has Wi-Fi 802.11n (150 Mbit/s) and an Ethernet connector, making it easier for the device to connect to the LAN network.

One of the most significant advantages of Raspberry Pi is excellent software support. There are many pre-compiled software packages and a large community of developers online.

In this study, three sensors have been used for measuring different parameters:

- Temperature and humidity sensor: The Sense HAT [28] has been used for measuring temperature and humidity in the secondary substation. The Sense HAT has an 8 × 8 RGB LED matrix, a five-button joystick, and includes the following sensors: (i) gyroscope (ii) accelerometer, (iii) magnetometer, (iv) temperature, (v) barometric pressure, and (vi) humidity.
- Voltage Sensor: A sensor module, namely ZMPT101B, has been used [29].
- Current Sensor: A ROGOWSKI coil has been used for measuring the current [30] (Fig. 1).

Table 1 Features of raspberry pi 3 B+ and raspberry pi 4 [27]

Features	Raspberry Pi 3 B +	Raspberry Pi 4
CPU	Broadcom BCM2837B0 Quad core Cortex-A53 @ 1.4 GHz	Broadcom BCM2711 Quad core Cortex-A72 @ 1.5 GHz
GPU	VideoCore IV @ 250-400 MHz	VideoCore VI @ 500 MHz
RAM	1 GB LPDDR2 SDRAM	1 GB, 2 GB or 4 GB LPDDR4-2400 SDRAM
USB	4 × USB-A 2.0 ports	2 × USB-a 2.0, 2 × USB-A 3.0, 1 × USB-C
Display port	Single full-size HDMI	2 × microHDMI
Connectivity	802.11ac Wi-Fi, 300Mbps Ethernet, Bluetooth 4.0	802.11ac Wi-Fi, Gigabit Ethernet, Bluetooth 5.0
Misc	40-pin GPIO header, 3.5-mm audio port, camera module support, composite video	40-pin GPIO header, 3.5-mm audio port, camera module support, composite video
Programming language	Python is desirable, and C, C + + ruby are preinstalled	Python is desirable, and C, C + + ruby are preinstalled

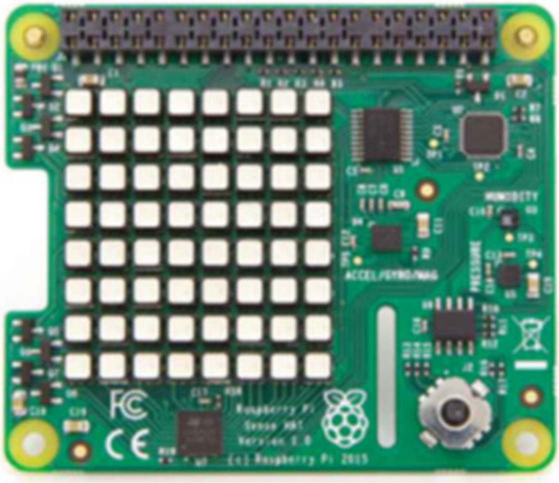


Fig. 1 Sense HAT sensor

The analog-to digital converter, named ADS1115, was implemented to convert the output signal of the sensors [31].

3 TLC Infrastructure

The Raspberry Pi 4 plays the role of a server that receives the measurement data in the form of strings and stores them for future use. Two Python codes were made in the Thonny IDE environment to provide the software required. The "client" code installed in Raspberry Pi 3 reads the measurement data incoming from the sensors, store the data for future use, connects to a given host IP address, and transfers the data in the form of strings via a socket communication. The "server" code establishes a socket communication, binds it to a given port number, and listens to incoming communication. The server receives the measurement data and stores it in the Raspberry Pi 4 storage SD card.

From a software point of view, the Raspberry Pi operating system Raspbian GNU/Linux 9 was adopted. The main benefit of the Raspberry Pi consists of the communication interfaces, such as the secure shell protocol (SSH) and virtual network computing (VNC) utilizing the remote frame buffer protocol (RFB). These may enable both remote wireless access to the PC and wired access to the PC, without the need of connection to a local network with the device to communicate with. In this study, Python programming has been used for measuring temperature and humidity. Socket programming was used to connect two network nodes so that they can interact with one another. One socket listens on a specific port at an IP address, while the other socket seeks to connect (Fig. 2).

The most common type of socket application is client–server applications, where one side acts as the server and waits for connections from clients. The server creates

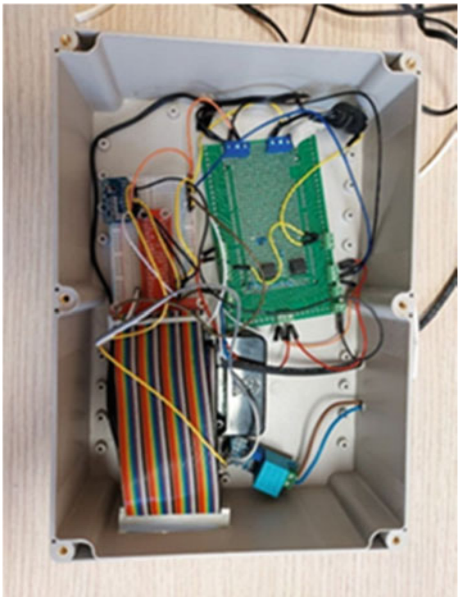


Fig. 2 Prototype system setup in the outdoor box

the listener socket, while the client connects to the server. The communication system based on TCP/IP socket communication consists of two sides: server and client. The client side is responsible for connecting to the server and transmitting the measured data to the server. The server side is responsible for establishing a socket connection and binding it to a port, receiving measurement data from the client, storing it in the memory of the single-board computer.

The details of the coding of both sides are as follows:

- The client-side Python code is made as follows: (i) defines all necessary libraries and variables, including host (server IP address) and port; (ii) defines functions responsible for reading the sensor measurements and for the communication with the server; (iii) defines a function that writes the measurements into a log file, where each string combines measured variables, date and time of measurement; (iv) then, another function encodes the string containing the measurement variables and sends them via socket communication established before; (v) the measuring, logging combining, encoding, and transmitting functions are put inside an infinite loop to ensure continuity. The measurement granularity is set at every 3 s.
- The server code consists of a series of functions that finally log the information received from the client. (i) The socket communication is created; (ii) it is bound with a pre-defined port number; (iii) the server starts listening to potential client requests; when the signal code is received, the server starts a loop. This loop continuously receives the information, decodes it with UTF-8 (by default), and (iv) logs it into a file opened previously. This file does not have a specific format, but the information received are comma-separated values (CSV).

A diagram representation of the IT infrastructure, described before, is shown in the following figure.

4 Case Study

As a case study, the metering device was installed in Terni DN, with the configuration shown in Fig. 3. ASM Terni grid is managed by its production unit Terni Distribuzione Elettrica (TDE), and it is characterized by three primary substations, feeding about 60 MV lines (at 10 and 20 kV), and about 700 secondary stations. The network extends for 2400 km, 25% of which is at MV level. The DSO is responsible for supplying about 400 GWh per year. More information can be found in [32–35]. In the case study, the device was used to measure ASM's headquarters power connection demand in the LV substation. ASM Terni headquarters comprise (i) a 4050 m^2 three-story office building; (ii) a 2790 m^2 single-story building consisting of technical offices, a computer center, and an operation control center, and (iii) a 1350 m^2 warehouse. The annual building consumption is about 650 MWh, mainly due to lighting, HVAC, and powering computers and data servers, and the district includes a 60 kW PV plant.

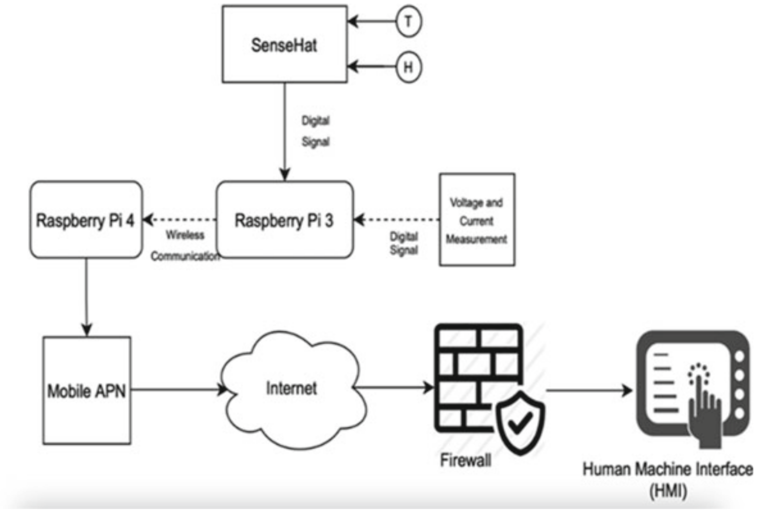


Fig. 3 IT infrastructure of the proposed monitoring device

An expansion board was considered to make the sensors accessible to the measurement place to realize the system, and an outdoor box was used to protect the systems from environmental hazards. For this project, the monitoring device was turned on for about one month, and then, the measurement data were collected via VNC remote control. The following figures illustrate the prototype device installed at the secondary substation at TDE DN. For installing the system in the secondary substation of TDE, an indoor box was used, as represented in Fig. 4.

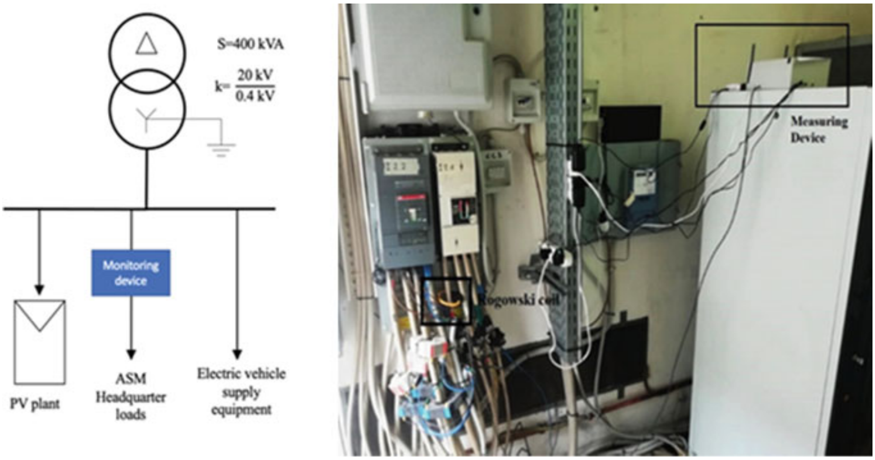


Fig. 4 Location of the measuring device in the terni electricity grid

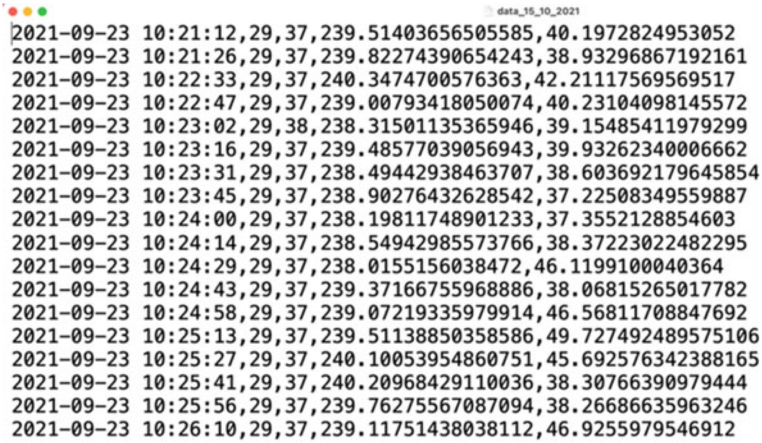
In the study, we used a laptop to control and monitor data obtained from a Raspberry Pi through a Wi-Fi connection to achieve the goal of remote-mode communication. As a result, joining the Raspberry Pi to a Wi-Fi network is possible by determining its IP address using a sophisticated IP scanner, and then, the graphical user interface is accessed using the virtual network computing (VNC) server software.

5 Results

An example of the acquired data in real time at the secondary substation of the ASM district is illustrated in Fig. 5.

As expressed in Section 2, measured data concern secondary substation temperature in °C, secondary substation humidity in %, RMS value of voltage, expressed in volt, at LV level for ASM district load and RMS value of current, expressed in ampere, at LV level for ASM district load.

As can be seen from Fig. 6, during the period under consideration the voltage is always between 242 and 231 V, i.e., in p.u. between 1.05 and 1.004. The current, on the other hand, varies more, ranging from around 30 A to almost 150 A. The acquired data concern the electrical quantities of the line connecting ASM's headquarters with the secondary substation; therefore, the trend of the curves is very jagged, due to variegate types of loads and the power generation from the PV system. The granularity of the data is 15 s, feasible to the DSR campaigns implementation.



```
2021-09-23 10:21:12,29,37,239.51403656505585,40.1972824953052
2021-09-23 10:21:26,29,37,239.82274390654243,38.93296867192161
2021-09-23 10:22:33,29,37,240.3474700576363,42.21117569569517
2021-09-23 10:22:47,29,37,239.00793418050074,40.23104098145572
2021-09-23 10:23:02,29,38,238.31501135365946,39.15485411979299
2021-09-23 10:23:16,29,37,239.48577039056943,39.93262340006662
2021-09-23 10:23:31,29,37,238.49442938463707,38.603692179645854
2021-09-23 10:23:45,29,37,238.90276432628542,37.22508349559887
2021-09-23 10:24:00,29,37,238.19811748901233,37.3552128854603
2021-09-23 10:24:14,29,37,238.54942985573766,38.37223022482295
2021-09-23 10:24:29,29,37,238.0155156038472,46.1199100040364
2021-09-23 10:24:43,29,37,239.37166755968886,38.06815265017782
2021-09-23 10:24:58,29,37,239.07219335979914,46.56811708847692
2021-09-23 10:25:13,29,37,239.51138850358586,49.727492489575106
2021-09-23 10:25:27,29,37,240.10053954860751,45.692576342388165
2021-09-23 10:25:41,29,37,240.20968429110036,38.30766390979444
2021-09-23 10:25:56,29,37,239.76275567087094,38.26686635963246
2021-09-23 10:26:10,29,37,239.11751438038112,46.9255979546912
```

Fig. 5 Data sample

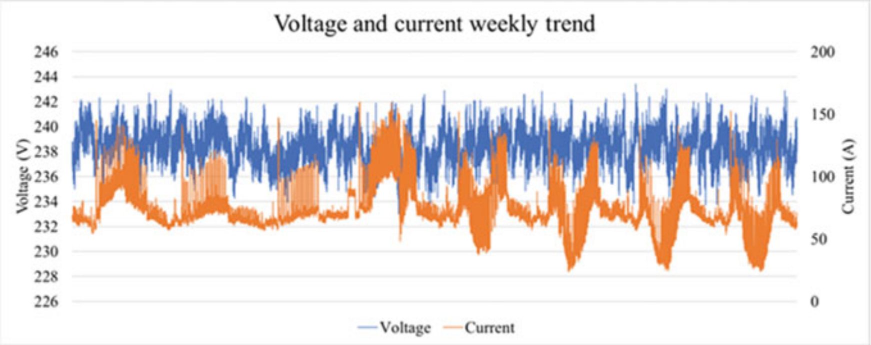


Fig. 6 Voltage and current measured at the ASM secondary station by the proposed monitoring device in the week of 24/09/2021–01/10/2021

6 Conclusion

The paper shows the realization of a simple and cost-effective monitoring device, easily applicable on a large-scale DN and whose data can be accessed just through a simple Internet connection. The implemented device was installed and tested within a secondary substation of ASM grid, monitoring the consumption of the ASM district for a short period of analysis.

A capillary knowledge of consumption/production profiles of LV/MV customers allows to enable the adoption of innovative strategies, which will play an increasingly important role in the energy transition. DSR and the implementation of flexibility tools, such as storage systems and smart electric vehicle charging stations, require the monitoring of the network in near real time.

The large-scale introduction of these technologies results extremely expensive for DSOs in case of adoption of complex monitoring infrastructure. Indeed, an economical, simple, and reliable device, such as the prototype presented in this article, could represent the optimal solution for enabling these new services, avoiding the possibility to carry on more accurate analysis that should require huge amount of data flow.

For future research, the authors are investigating the possibility to increase the adoption of such devices in ASM DN also implementing AI-based and machine learning tools for analytics purposes. In addition, the amount of data to be transmitted will be discussed, trying to adopt some techniques to limit the flow of data to be transmitted to the DSO.

Acknowledgements This project has received funding from the European Union's Horizon 2020 research and innovation program under the IoT-NGIN project grant agreement No 957246.

References

1. Ardito L, Procaccianti G, Menga G, Morisio M (2013) Smart grid technologies in Europe: an overview. Energies 6(1):251–281. https://doi.org/10.3390/EN6010251
2. Sechilariu M, Wang B, Locment F (2013) Building-integrated microgrid: advanced local energy management for forthcoming smart power grid communication. Energy Build 59:236–243. https://doi.org/10.1016/J.ENBUILD.2012.12.039
3. Li F et al (2010) Smart transmission grid: vision and framework. IEEE Trans Smart Grid 1(2):168–177. https://doi.org/10.1109/TSG.2010.2053726
4. Siano P (2014) Demand response and smart grids—a survey. Renew Sustain Energy Rev 30:461–478. https://doi.org/10.1016/j.rser.2013.10.022
5. Fang X, Misra S, Xue G, Yang D (2012) Smart grid—the new and improved power grid: a survey. IEEE Commun Surveys Tutorials 14(4):944–980. https://doi.org/10.1109/SURV.2011.101911.00087
6. Deblasio R, Tom C (2008) "Standards for the smart grid." In 2008 IEEE energy 2030 conference, pp 1–7
7. Sha K, Alatrash N, Wang Z (2021) "A secure and efficient framework to read isolated smart grid devices". IEEE Trans Smart Grid 8(6). Accessed 04 Oct 2021. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.uniroma1.it/document/7419260/
8. Morello R, de Capua C, Fulco G, Mukhopadhyay SC (2017) A smart power meter to monitor energy flow in smart grids: the role of advanced sensing and iot in the electric grid of the future. IEEE Sens J 17(23):7828–7837. https://doi.org/10.1109/JSEN.2017.2760014
9. Sharma K, Mohan Saini L (2015) Performance analysis of smart metering for smart grid: an overview. Renew Sustain Energy Rev 49:720–735. https://doi.org/10.1016/J.RSER.2015.04.170
10. Uludag S, Lui KS, Ren W, Nahrstedt K (2026) "Secure and scalable data collection with time minimization in the smart grid." IEEE Trans Smart Grid 7(1). Accessed 04 Oct 04 2021. [Online]. Available: https://ieeexplore.ieee.org/document/7061965/
11. Samson JB, Fredrick KA, Sathiya MN, Joy RC, Wesley WJ, Samuel SS (2019) "Smart energy monitoring using raspberrypi." Accessed 04 Oct 2021. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.uniroma1.it/document/8819743/
12. Ashok K, Li D, Divan D, Gebraeel N (2020) "Distribution transformer health monitoring using smart meter data." Accessed 04 Oct 2021. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.uniroma1.it/document/9087641/
13. Kunicki M, Borucki S, Zmarzły D, Frymus J (2020) Data acquisition system for on-line temperature monitoring in power transformers. Measurement 161:107909. https://doi.org/10.1016/J.MEASUREMENT.2020.107909
14. Moghaddass R, Wang J (2018) "A hierarchical framework for smart grid anomaly detection using large-scale smart meter data." IEEE Trans Smart Grid 9(6). Accessed 04 Oct 2021. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.uniroma1.it/document/7908945/
15. Cataliotti A, Cosentino V, di Cara D, Tinè G (2016) "LV Measurement device placement for load flow analysis in mv smart grids." IEEE Trans Instrument Measure 65(5). Accessed 04 Oct 2021. [Online]. Available: https://ieeexplore.ieee.org/document/7321815/
16. Albu MM, Sănduleac M, Stănescu C (017) "Syncretic Use of smart meters for power quality monitoring in emerging networks." IEEE Trans Smart Grid 8(1). Accessed 04 Oct 2021. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.uniroma1.it/document/7536160/
17. Elma O, Selamoğullari US (2017) "An overview of demand response applications under smart grid concept." Accessed 05 Oct 2021. [Online]. Available: https://ieeexplore.ieee.org/document/7935802/
18. Samad T, Koch E, Stluka P (2016) "Automated demand response for smart buildings and microgrids: the state of the practice and research challenges." Proc IEEE 104(4). Accessed 05 Oct 2021. [Online]. Available: https://ieeexplore-ieee-org.ezproxy.uniroma1.it/document/7416149/

19. Bahrami S, Sheikhi A (2016) “From demand response in smart grid toward integrated demand response in smart energy hub.” IEEE Trans Smart Grid 7(2). Accessed 05 Oct 2021. [Online]. Available: https://ieeexplore.ieee.org/document/7206579/
20. Ko W, Vettikalladi H, Song SH, Choi HJ (2020) Implementation of a demand-side management solution for South Korea’s demand response program. Appl Sci 10(5):1751. https://doi.org/10.3390/APP10051751
21. Hoosain MS, Paul BS (2017) “Smart homes: a domestic demand response and demand side energy management system for future smart grids.” Accessed 05 Oct 2021. [Online]. Available: https://ieeexplore.ieee.org/document/7931852/
22. Latifi M, Khalili A, Rastegarnia A, Bazzi WM, Sanei S (2020) A robust scalable demand-side management based on diffusion-admm strategy for smart grid. IEEE Internet Things J 7(4):3363–3377. https://doi.org/10.1109/JIOT.2020.2968539
23. Minchala-Avila LI, Armijos J, Pesántez D, Zhang Y (2016) Design and implementation of a smart meter with demand response capabilities. Energy Procedia 103:195–200. https://doi.org/10.1016/J.EGYPRO.2016.11.272
24. Li WT et al (2015) Demand response management for residential smart grid: from theory to practice. IEEE Access 3:2431–2440. https://doi.org/10.1109/ACCESS.2015.2503379
25. IoT-NGIN European Project website https://iot-ngin.eu
26. Merchant HK, Ahire DD (2017) “Industrial automation using IoT with raspberry pi,” 2017
27. Raspberry Pi website, https://www.raspberrypi.com
28. Sensor Hat description, https://projects.raspberrypi.org/en/projects/getting-started-with-the-sense-hat
29. Voltage sensor description, https://innovatorsguru.com/zmpt101b/
30. Rogowski coil description, https://www.cnzentar.com/rogowski-coils/?gclid=CjwKCAjwwsmLBhACEiwANq-tXKDMavNPLVIz2TVIOqsaK8QKpUp44rHFiRSL4Hd8rZi0_iQ27qbRoCrL4QAvD_BwE
31. ADS1115 analog to digital converter description, https://www.adafruit.com/product/1085
32. Carere F et al (2020) “Flexibility—enabling technologies using electric vehicles.” In 2020 IEEE international conference on environment and electrical engineering and 2020 IEEE industrial and commercial power systems Europe (EEEIC/I&CPS Europe), pp 1–6. https://doi.org/10.1109/EEEIC/ICPSEurope49358.2020.9160781.
33. Carere F et al (2021) Electric vehicle charging rescheduling to mitigate local congestions in the distribution system. IEEE Madrid PowerTech 2021:1–6. https://doi.org/10.1109/PowerTech46648.2021.9494882
34. Koukaras P, Gkaidatzis P, Bezas N, Bragatto T, Carere F, Santori F, Antal M, Ioannidis D, Tjortjis C, Tzovaras D (2021) A tri-layer optimization framework for day-ahead energy scheduling based on cost and discomfort minimization. Energies 14:3599. https://doi.org/10.3390/en14123599
35. Antal C, Cioara T, Antal M, Mihailescu V, Mitrea D, Anghel I, Salomie I, Raveduto G, Bertoncini M, Croce V, Bragatto T, Carere F, Bellesini F (2021) “Blockchain based decentralized local energy flexibility market”. Energy Reports 7:5269–5288, ISSN 2352–4847, https://doi.org/10.1016/j.egyr.2021.08.118

Investigating the Sinkhole Attack in Cognitive Wireless Sensor Network

Zenzele Malale, Mthulisi Velempini, and Sekgoari Semaka Mapunya

Abstract Wireless sensor network (WSN) is a network that senses its environment, collects data, and routes data to sink node through wireless links. However, security is a challenge. Sinkhole attack is one of the main security issues that threatens the operation of WSN. Sinkhole nodes advertise themselves as best link route to the base station for malicious reasons. Thereafter, the attacker drops packets and modifies data, enabling other attacks such as selective forwarding and worm-hole attacks to be launched. This study focusses on investigating the effectiveness of sinkhole attack mitigation schemes in cognitive WSN and designed a framework for future research. MATLAB simulation tool was utilized to simulate and evaluate the sinkhole attack mitigation schemes, and comparative results were generated. The metrics which were considered in the simulation are the packet delivery ratio, probability of detection, and the probability of false alarm. The results show that the mitigation of sinkhole attacks requires further attention.

Keywords Mitigation · Selective forwarding · Sinkhole attack · Wireless sensor networks · Worm-hole attacks

1 Introduction

The main purpose of this study is to investigate the performance of sinkhole attack schemes in wireless sensor network (WSN). WSN is a network that senses network environment, collects data, and sends data wirelessly to the sink node [1]. However, an attack known as the sinkhole attack compromises the routing technique by advertising itself as the best route to the base station [2]. The objective of the attack is to either drops packets or modify them for malicious purposes. The neighboring nodes then

Z. Malale · M. Velempini · S. S. Mapunya (✉)
Department of Computer Science, University of Limpopo, Mankweng, South Africa
e-mail: sekgoari.mapunya@ul.ac.za

M. Velempini
e-mail: mthulisi.velempini@ul.ac.za

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_53

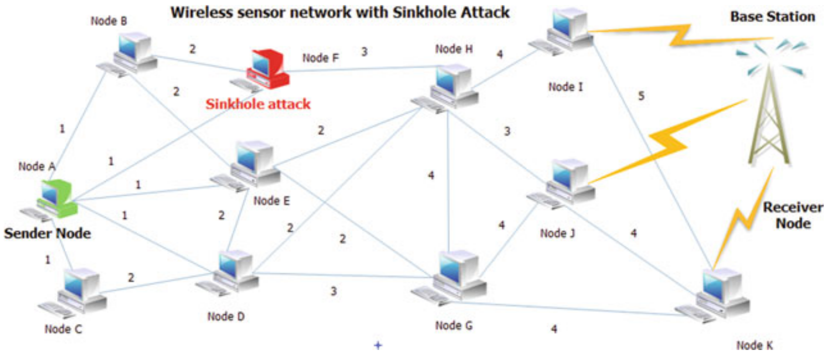


Fig. 1 Effects of a sinkhole attack

send their packets through the sinkhole node despite the fact that it is not the best route.

Figure 1 depicts a sinkhole node attack in WSN. The network is having one base station and a number of sensor nodes with their associated hop counts shown. The minimum and maximum hop count values range from 1 to 4. The nodes can communicate with their respective neighbors and relay packets. The packets are transmitted when a shortest route to the receiver has been identified. There is a sensor node A which wants to send a message to the base station. The sinkhole node F then advertises itself as the shortest route to the base station. The sinkhole node then receives packets from its neighborhood and drops them. The sinkhole node can also modify the packets before relaying them.

Given the adverse effects of the sinkhole node in the WSN, schemes have been proposed in literature with the main objective to detect and address the effect of the sinkhole attack. In this study, we do a comparative study of the following schemes: anomaly-based [3], hop count [4], and hybrid-based [5] schemes.

The study observed that the anomaly-based approach was able to detect the sinkhole attack; however, the scheme is optimized for the static wireless sensor network. The scheme is less efficient and has a high false-positive rate when there is a high packet drop rate. The key management scheme does not address the effects of the sinkhole node. However, it was designed to prevent the sinkhole attack. Our investigation shows that the hybrid-based approach is more efficient, and it also counters the effects of the sinkhole node. The hop count is more effective when the malicious node is not in the neighborhood of the base station. As a result, a sinkhole node which is within one hop of the base station cannot be detected. The comparative results were obtained through simulations using MATLAB simulating tool installed on Windows 10.

2 Related Work

In this section, we present and analyze schemes designed to mitigate the effects of sinkhole attack. In [4], an algorithm which detects suspicious nodes by analyzing the consistency of their data is proposed. Malicious nodes are further detected through the network flow data. The effectiveness of the proposed algorithm was evaluated using numerical analysis and simulations. However, the accuracy and efficiency of the scheme were not evaluated.

In [5], a cryptographic method which restrains the sinkhole attack in a tree-based routing structure in a wireless sensor network is proposed. Nodes are secured using a public key infrastructure which authenticate incoming messages and verify whether they are coming from the base station. Public keys and private keys are used to authenticate and to lock and unlock the data. The technique ensures that malicious nodes do not hide their identification. However, this method does not detect and eliminate the sinkhole attack. Lastly, the scheme is also effective where there is node collusion.

An algorithm which can detect sinkhole attack and identified an intruder is proposed in [6]. The scheme is statistical based and can differentiated between the malicious and the legitimate nodes faster and reduced the false-positive rate. However, the base station is the final decision maker whether a node is malicious or not. This means that when the scheme is launched, it does not detect the attack immediately.

The anomaly-based detection proposed in [7] employs a message digest algorithm to detect a sinkhole node using the one-way hash chains. The algorithm also ensures the data integrity of the messages transferred using the trustable and authentic paths. In the event of node collision, its performance is degraded. The performance of the proposed algorithm was evaluated through simulations which confirmed the efficiency of the algorithm in terms of success rate, false-positive rate, and false-negative rate when compared to other schemes.

In [4], authors proposed a hop count-based scheme to detect the sinkhole attack in WSN. The scheme was designed to function in the scenario where the network comprises of one base station. As the packets are relayed to the base station, the number of hops is counted. Nodes with hop counts which suggest that they are closer to the base stations are marked as malicious nodes. Unfortunately, not all nodes closer to the base station are ~~not~~ malicious. Secondly, malicious nodes with one hop away or two hops away from the base station cannot be detected.

In [8], a received signal strength indicator (RSSI) detection scheme is proposed. RSSI is used to measure the signal strength of nodes. The scheme uses the RSSI value with the support of extra monitor (EM) node to detect the sinkhole attack. The EM node monitors and analyze the network traffic. The RSSI value from EM nodes is used to determine the position of base station. However, false-positive and false-negative rate increases when packets are being dropped. The scheme cannot immediately detect malicious nodes soon after deployment, and lastly, it is optimized for static network.

Link quality indicator (LQI) is an anomaly-based scheme which measures the error in the packets which are received. This scheme was proposed by Choi. et al. in [9] which detects a sinkhole attack using LQI. The scheme suffers from high probability of false positive caused by the abnormal change of the values of the tolerant threshold.

Authors in [3] proposed a sinkhole dictation scheme. The scheme ensures that nodes do not share incorrect distance to the base station. However, it is very expensive to implement. The scheme is a hop by hop which depends on a tree-based structure.

In rule-based detection, predefined rules are used to check whether data points are classified as normal or anomalous. The algorithm detects intrusion using monitor nodes for the wireless sensor network. If there are any malicious nodes that will violate the rules, then they will be discarded from the network with immediate effect since all nodes are expected to follow the rules.

Krontiris et al., in [10], proposed a rule-based scheme which notifies the legitimate nodes of any existing of attackers. The scheme is twofold, rule based, and a complimentary intrusion detection alarm which is activated when the rule-based part fails. The scheme can detect malicious nodes though it cannot identify the identity of the node.

A hybrid-based detection is a scheme that combines two detection techniques. Anomaly and misuse detection schemes can be combined where statistically and anomaly techniques are used for detection. In [5], an intrusion detection system which combines both the signature based and the anomaly approaches was proposed. The scheme detects malicious nodes and isolate them.

Redundancy is a technique where data are sent in multiple paths and be saved in different systems to increase high availability of data in the event of security attacks. In [11], a detecting scheme which sends data using more than one route was proposed.

Mohammad Wazid et al. in [12] designed a detection mechanism for the hierarchical wireless sensor network. The scheme detected the nodes that drop packets, nodes that delay the packets, and those which modify packets. The scheme is cluster based and was simulated in NS2, and the results show that the scheme achieved 95% probability of detection. In [13], an efficient and secure protocol for the heterogeneous sensor network was proposed. The scheme implemented high-end sensors, and the routing performance has proven to be effective for the heterogeneous sensor network. The packet delivery rate decreases as the number of failure nodes increases. Dallas et al. in [14] proposed a method that can detect the sinkhole attack or any kinds of attack in the wireless sensor network which monitors the hop count values of the nodes and observe any abnormal route advertisement.

3 Simulation Environment

The hybrid algorithm in [15] implements two methods to detect the sinkhole attack, namely: leader-based monitoring and zone-based leader election method. The cluster-based zone allocation (CBZA) [16] divides zones into four regions with

Table 1 Database table of the nodes

Node ID	N1	N2	N3	N4	N5	N…	N*i*
Location	1,2	2,4	5,3	3,2	6,9	…	*i,j*

a cluster head (CH). In the leader-based monitoring mechanism [17], a leader is chosen for monitoring the network and deal with any malicious behavior. Every region in the network is allocated a cluster-based zone leader (CBZL) which was proposed by Rajkumar et al. in [17]. The CH collects data from all nodes, and the base station then analyzes data. Each node had a node ID table to store the ID node value and the location. The data in Table 1 were used to authorize nodes before they could communicate.

A particular zone is selected, and within the zone, the energy levels of nodes are compared such that the node with the highest energy level is selected as a zone leader. To detect an attacker, Eq. 1 was used.

Intrusion ratio (IR) equation

$$\mathrm{IRj} = \frac{\mathrm{PRj}}{\mathrm{PTj}} \tag{1}$$

where PRj is the packet reception value and PTj *is the* packet transmission value. If the value of IRJ is equal to a numeric value, then it implies that the packets are not dropped and that there is no sinkhole attack; however, if IRJ is equals to infinity, then it is considered that the malicious node had dropped some packets which is associated with a black hole. Secondly, if the difference between PRj and PTj is significant difference, then it is assumed that there is a possibility of selective forwarding attack. The information is shared in the network, and the attacking nodes are isolated. According to literature, the scheme is best performing and detects 80% of the attacks.

The hop count considered a sensor network with one base station, and the nodes were located randomly. The nodes are able to communicate and send data to the base station using hop-by-hop method. All nodes are uniquely identified and are static. The base station broadcasts hello packets to establish hope counts of nodes and their IDs as depicted in Table 2.

A message is broadcasted to neighboring nodes when the sinkhole attack has been detected. A node whose value is greater than 40% which is the threshold value, the

Table 2 Hop counts and identity of nodes

Node ID	Hop count
12	4
14	5
21	5
18	5

node is classified as a malicious node. The success rate was determined by the number of the neighbor nodes that was able to detect the malicious nodes. If the neighbor node could not detect the malicious node, the scheme is considered unsuccessful [4]. The performance of the scheme was based on the number of neighboring nodes which are able to detect the attack.

3.1 Simulations

The MATLAB simulation tool was used for simulation. The simulator is popular with many researchers in this field of research. The MATLAB was run in windows operating system, Windows 10 operating system.

We considered three scenarios of networks with 10, 25, 50, 75, and 100 nodes. The number of sinkhole nodes was considered to range from 10%, 20% to 30% to effectively evaluate the detection schemes. We first considered a network with 50 nodes without a sinkhole attack. The performance of the schemes was evaluated using the following metrics: packet delivery ratio, probability of detection (Pd), and the probability of false alarm (Pf) using the following equations:

$$packet\ delivery\ ratio = \frac{\text{received packet}}{\text{sent a packet}} \tag{2}$$

$$Pd = \frac{\text{detected target}}{sum\ of\ all\ possible\ targets\ in\ a\ given\ direction} * 100\% \tag{3}$$

$$\text{Pf} = 1 - \text{pd} = 1 - \frac{dt}{\sum all\ possible\ targets} \tag{4}$$

Table 3 presents simulation parameters with their respective values used in this study to evaluate the security schemes.

4 Results

In this section, we present and discuss the comparative results of the security schemes we evaluated. The first set of results is based on the performance of the schemes in terms of the detection rate. In Fig. 2, the probability of detection results of scenarios with 10, 20, and 30% of malicious nodes in different network sizes is shown. In a network with ten nodes, the rate of the probability of detection is 1 which means that all the schemes were able to detect all the attacks. However, as the percentage of the sinkhole attack nodes increased, the detection schemes were degraded. The hybrid-based detection scheme was superior to the anomaly and hop count-based detection

Table 3 Simulation parameters

Simulation tool	Example
Simulation tool	MATLAB
Operating system	Windows 10
Number of nodes	10, 25, 50, 75, 100
Number of sinkhole	10%, 20%, 30%
Simulation time	300 s
Number of base station	1
Routing protocol	An on-demand distance-vector routing protocol
Network environment	Hybrid
Sensing type	Energy detection
Grid size	1000 m * 1000 m
Channel data rate	11 M bits/s
Nodes type	Mobile Nodes
Parameter	Setting
Antenna type	OmniAntenna
MAC protocol	IEEE 802.11b CR networks capabilities
Metrics	Packet delivery ratio The probability of false alarm Probability of detection

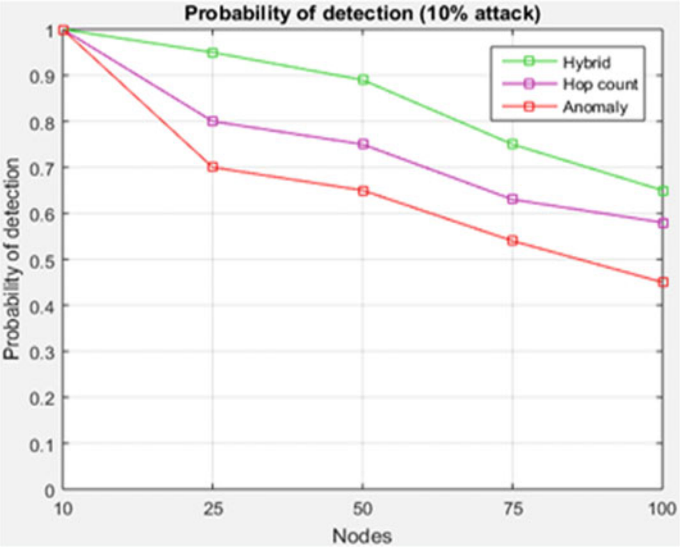


Fig. 2 Probability of detection in a network with 10% of nodes being sinkholes

scheme. The anomaly-based detection scheme was worst because it is optimized for static networks, and it requires more monitor nodes.

The results of a network with 10% of nodes being sinkhole nodes are shown in Fig. 2. The schemes performed well in a scenario without sinkhole nodes. However, as the size of the networks was increased to 25 with 10% attacking nodes, the performance of the schemes ranged from 70 to 96%. In a network with 50 nodes and 10% attacking nodes, the performance ranged from 65% to 90%. The hybrid scheme was observed as the best performing scheme. It can also be seen that as the number of nodes increased in the presence of malicious nodes, the performance of the schemes was degraded. For example, when the nodes were 100, the detection rate was degraded to 46 and 65%. Figure 3 shows the results of the hybrid, hop count, and anomaly-based detection schemes with 20% of malicious nodes.

In Fig. 3, the probability of detecting 25 nodes with 20% of the attack is ranged between 65 and 82%. As the number of nodes increased to 100, the performance of the scheme ranged between 30 and 42%.

The results of the probability of detecting in a scenario with 30% malicious nodes are shown in Fig. 4. The performance of the schemes is ranged between 55 and 73%. As the size of the network increased to 100 nodes, the performance of the schemes degraded to between 30 and 42%.

Figure 5 shows the comparative probability of false alarm results. The probability of false alarm is the probability misdetection. The results show that schemes were subjected to low probability of false alarm with the hybrid detection scheme achieving the worst results.

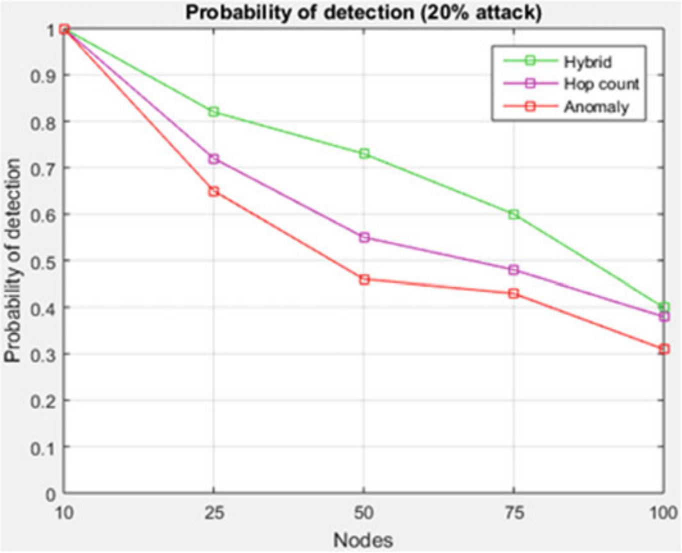


Fig. 3 Probability of detection in a network with 20% of nodes being sinkholes

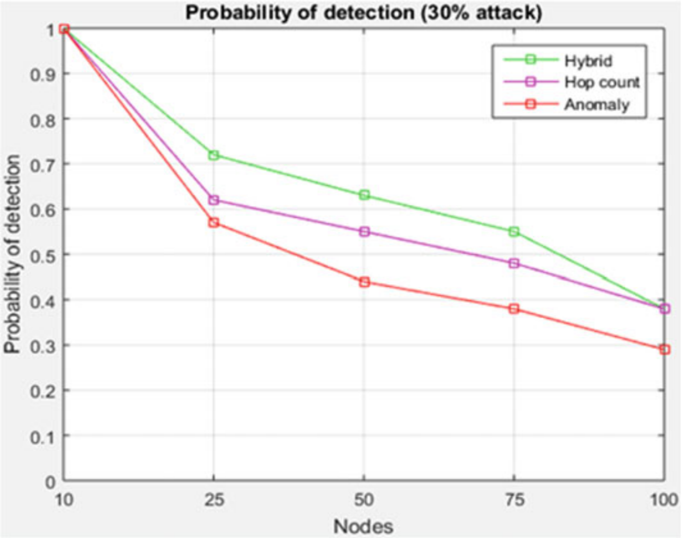


Fig. 4 Probability of detection in a network with 30% of nodes being sinkholes

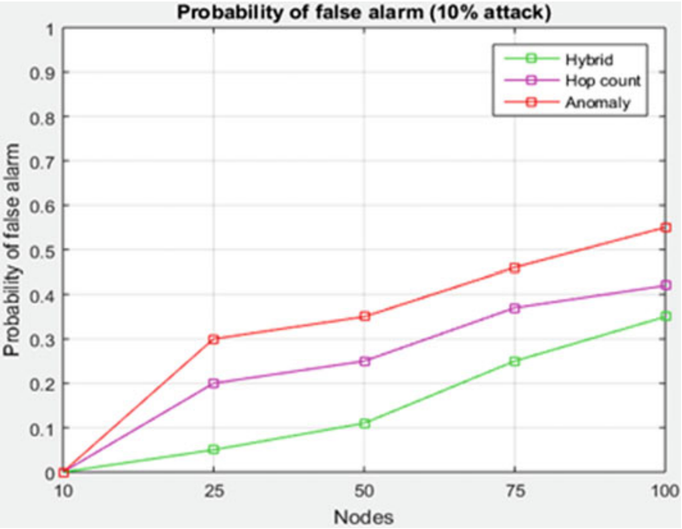


Fig. 5 Probability of false alarm in a network with 10% of sinkhole nodes

The probability of false alarm in networks with 10–100 nodes and 10% malicious nodes is shown in Fig. 5. The anomaly-based scheme achieved the best results. The hop count had 20% probability of false alarm in network with 25 nodes, while the hybrid scheme had 5%. However, as the nodes increased, the schemes were degraded.

Figure 6 shows the results of the detection scheme in a network with nodes ranging from 10 to 100 nodes with 20% of sinkhole nodes. In a scenario with 25 nodes, the false alarm ranged from 19 to 35%. However, when the nodes were increased to 50, the hybrid had 29%. The anomaly-based scheme was the worst scheme with 54%, while the hop count had 45%. The performance of the schemes worsened when the number of nodes was increased to 100. The probability of false alarm results ranged between 60 and 70%. This shows that the performance of the schemes is degraded by the increase in the number of nodes and the presence of the sinkhole nodes.

Figure 7 clearly shows the impact of the network size and the number of malicious nodes on the performance of the network. As the number of both nodes and sinkhole nodes increased in the network, the performance of the schemes further degraded. In Fig. 7, the number of sinkhole nodes was increased to 30% of the total number of nodes in the network. The anomaly-based scheme had the worst performance, while the hybrid scheme had the best performance.

The results in Fig. 8 clearly show how the sinkhole attack impacts negatively on the performance of the network. The performance of the network degraded as the number of nodes was gradually increased. In this case, it degraded with time. In a network with 30 nodes in Fig. 8, only, 94% of the sent packets was delivered by the hybrid scheme. The hop count delivered 80%, while the anomaly delivered 60%. The performance of the schemes worsened with time as shown in Fig. 8.

Figure 9 shows the results of the packet delivery metric that was used to check the performance of the hybrid, anomaly, and hop count base scheme. The result is analyzed with the number of 30 packets sent to the base station. Due to the sinkhole attack distracting the network, more packets were dropped.

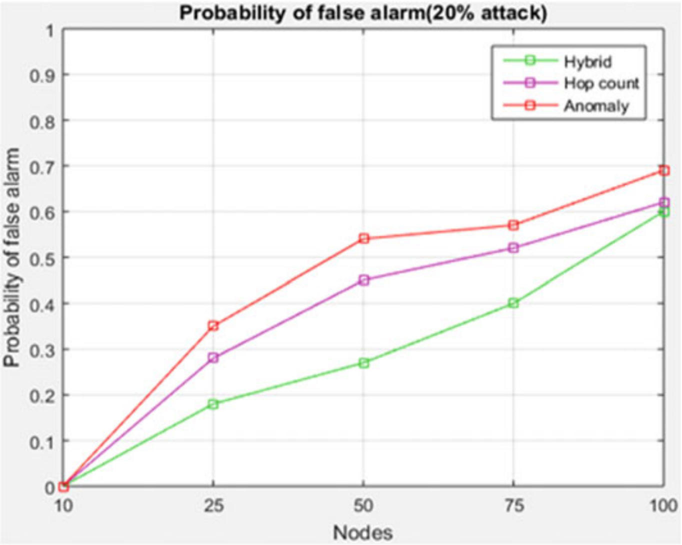


Fig. 6 Probability of false alarm in a network with 20% of sinkhole nodes

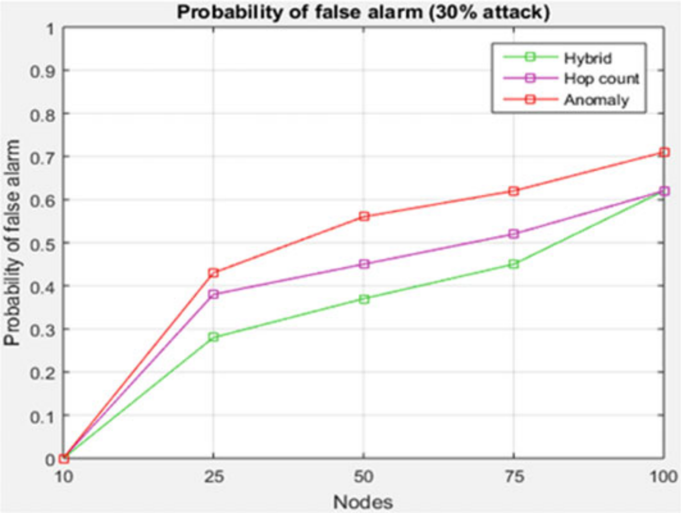


Fig. 7 Probability of false alarm in a network with 30% of sinkhole nodes

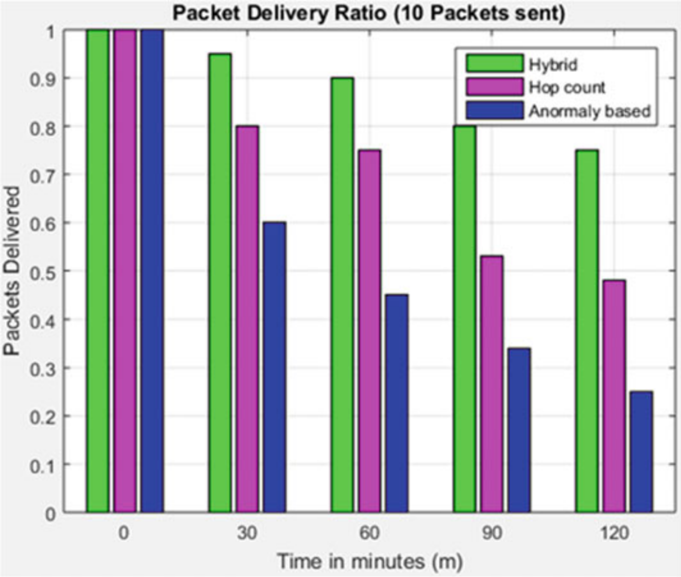


Fig. 8 Packet delivery ratio of the schemes where ten packets were transmitted

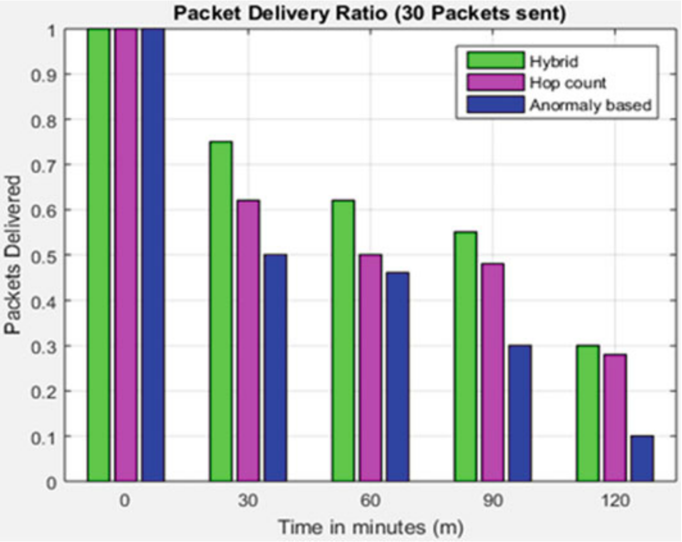


Fig. 9 Packet delivery ratio of the schemes where 30 packets were transmitted

The results in Fig. 9 show that the hybrid scheme outperformed the other two schemes. However, all the three schemes dropped more packets with time. Furthermore, an increase in the number of packets sent to the base station also impacted negatively on the performance of the network. As we increase the number of packets in the network, we observed that the probability of the packets being delivered decreased. The increase in the packet drop rate is caused by the presence of the sinkhole nodes. The anomaly-based detection scheme was the least performing scheme as can be observed in Fig. 10.

We can conclude that an increase in the number of nodes, packets sent, and malicious nodes causes the efficiency of the detection schemes to degrade. In the scenarios considered, the hybrid is the best performing scheme in comparison to the anomaly and hop count-based detection schemes. An integration of the hybrid, anomaly-based, and the hop count schemes may achieve a best performing scheme. The integration may endeavor to design a new scheme based on the best feature of the three schemes.

5 Conclusion

The paper provided an in-depth analysis of the sinkhole attack and the existing sinkhole attack detection schemes. This will enable researchers to design efficient detection scheme based on the best attributes of the evaluated schemes: the hybrid detection, the hop count, and the anomaly schemes. The hop count-based scheme

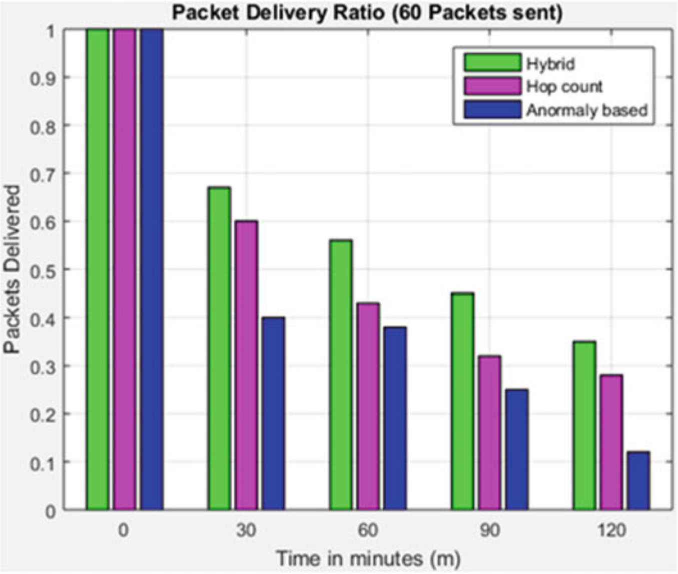


Fig. 10 Packet delivery ratio of the schemes where 60 packets were transmitted

detects the attack based on the routing table of the neighboring nodes. The identification of the neighboring nodes and the hop count value of the nodes is therefore key to ensuring the efficiency of this scheme. The anomaly-based detection scheme detects the attack based on abnormal network traffic that the sinkhole diverts to a given node, the sinkhole node. However, the hybrid of the two or more techniques has shown to be more effective which can inform future research direction.

References

1. Sweta J, Pruthviraj C, Ayushi S (2021) "The fundamentals of internet of things: architectures, enabling technologies, and applications." In Healthcare paradigms in the internet of things ecosystem, ScienceDirect, pp 1–20
2. Pradeepkumar B, Sukanta D, Santosh B, Sukumar N (2019) "Energy efficient approach to detect sinkhole attack using roving IDS in 6LoWPAN network." In International conference on innovations for community services, Springer, pp 187–207
3. Chanatip T, Ruttikorn V (2010) "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks." In 2009 7th international conference on information, communications and signal processing (ICICS), Macau, China
4. Ibrahim AM, Mohammad MR, Mukul CR (2015) Detecting sinkhole attacks in wireless sensor network using hop count. Int J Comput Netw Inf Secur (IJCNIS) 7(3):50–56
5. Luigi C, Salvatore D, Luigi R, Gianluigi S (2010) "An intrusion detection system for critical information infrastructures using WSN technologies." In 2010 5th international conference on critical infrastructure (CRIS), An intrusion detection system for critical information infrastructures using WSN technologies

6. Chen C, Song M, Hsieh G (2010) "Intrusion detection sinkhole attack in large scale wireless sensor network. In Wireless communication, networking and information security (WCNIS)," in IEEE Interational Conference
7. Sharmila S, Umamaheswari G (2011) "Detection of sinkhole attack in wireless sensor networks using message digest algorithms." In 2011 international conference on process automation, control and computing
8. Tumrongwittaya, Varakulsiripunth (2009) "Detection of sinkhole attack in wireless sensor networks." In ICCAS-SICE, pp 1966–1971, IEEE
9. Byung GC, Eung JC, Jin HK, Choong SH, Jin HK (2008) "A sinkhole attack detection mechanism for LQI based mesh routing in WSN." In 2009 international conference on information networking, Chiang Mai, Thailand
10. Krontiris I, Giannetsos T, Dimitriou T (2008) "Launch sinkhole attack in wireless sensor network; the intruder side." In Networking and communications, 2008. WIMOB'08. IEEE international conference on wireless and mobile computing, pp 526–531
11. Zhanga FJ, Li-Dong Zhaia B, Jin-Cui Y, Xiang C (2014) "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks." In Procedia computer science 31, Beijing
12. Mohammad W, Ashok DK, Saru K, Muhammad KK (2016) "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks." Secur Commun Networks 4596–4614
13. Xiaojiang D, Mohsen G, Yang X, Hsiao-Hwa C (2007) Two tier secure routing protocol for heterogeneous sensor networks. IEEE Trans Wireless Commun 6(9):3395–3401
14. Dallas D, Leckie C, Ramamohanarao K (2007) "Hop-count monitoring: detecting sinkhole attacks in wireless sensor networks." In 15th IEEE international conference on networks (ICON 2007), Adelaide, Australia, 176–181
15. Udaya SR, Rajamani V (2015) A hybrid zone based leader for monitoring sinkhole attack in wireless sensor network. Indian J Sci Technol 8(23):1–9
16. Varma A, Aswani KR, Ravi TY, Thangavelu A (2015) Cluster based multipath dynamic routing (cbdr) protocol for wireles sensor networks. Indiana J Sci Technol 8(S2):17–22
17. Udaya SR, Rajamani V (2013) A leader based monitoring approach for sinkhole attack in wireless sensor network. J Computer Sci 9(9):1106–1116

A Novel Software Architecture to Calculate Effort Estimation for Industrial Big Data

Sadia Khan and Ammad Adil

Abstract Software development effort estimation is one of the main sub-disciplines of software cost estimation, which comes under software project management. To estimate effort accurately, we noted different estimation models. With the combination of expert judgment, data mining, and machine learning, the motive of this study is to propose a new software architecture for effort estimation. The proposed architecture uses techniques such as expert judgment along with K-means clustering and machine learning techniques such as ANN, SVR, LR, RF, and KNN. At last, we used RMSE, MAE, MMRE, and Pred (.25). After the experimentation, we noted the increase in estimation accuracy was seen with the use of the proposed estimation model. Moreover, support vector regression outperformed all other algorithms with $K = 3$ and 5 and expert input. Therefore, we concluded the effort estimation of industrial big data is an important step and needs to be given attention in software organizations.

Keywords Software architecture · Industrial big data · Effort estimation

1 Introduction

Data mining is an active area in the arena of software development effort estimation (SDEE) [1]. Despite the fact, plenty of work has been performed in the field of effort estimation; however, software development organizations are yet anxious and trying to reduce estimation error [2]. At present, vogue has been altered, and data are assembled from software development organizations for producing software development effort estimations [3]. For effort estimation, among all, the top used technique is expert judgment [4]. Though expert judgment could be flawed or flawless [5], the cause persists to be the unfairness of human experts.

With every new day, the software projects are increasing, and consequently, the size of the repository for software projects has also increased. The big data for

S. Khan (✉) · A. Adil
COMSATS University Islamabad, Islamabad Campus, Islamabad, Pakistan
e-mail: sadiakhan971@gmail.com

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_54

software-developed projects have been targeted in this study. As the increased number of software projects [6] and dataset sizes correspond to big data [7]. Therefore, we collected the software-industrial big data software industry located in Islamabad–Pakistan. Then, we re-organized this information to form dataset. Then, we re-shuffled this information to form dataset. After the construction of the dataset, initially, we applied a data mining technique named clustering. On the formed clusters, we applied machine learning algorithms such as random forest, support vector machines using the polynomial kernel, k-nearest neighbor, neural networks with ADAM problem solver, and linear regression with elastic net regression with the help tool named Orange. Consequently, this paper delivers an estimation architecture that adjusts well in the environment of software development effort estimation situated in the region of Islamabad–Pakistan. This architecture could lessen estimation error as compared to experts individually.

As an outcome, the architecture that we have built reduces the estimation error when compared with experts individually. In an actual environment of software development organizations, according to the work of [8], estimators could utilize the proposed architecture for effort estimation for robust results.

The remainder of this paper is assembled as methodology being part of Sect. 2. Section 3 comprises of results. Furthermore, conclusions and future works are presented in Sect. 4.

2 Methodology

The proposed framework presented in Fig. 1 is explained in this section. We conducted this experiment for two software development organizations. These organizations exceed 35 staff members that have been allocated with different responsibilities. Within software development organizations, we have seen wide use of

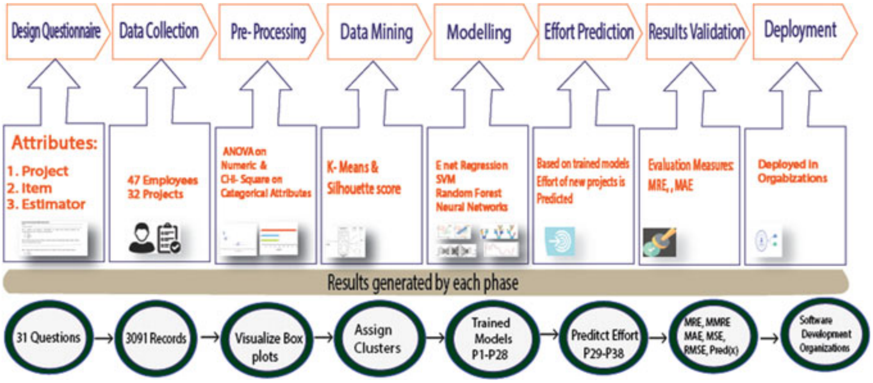


Fig. 1 Proposed software architecture for effort estimation

expert judgment. The data of already completed projects can be helpful in making estimations as suggested in the work of Minku [9–11]. Therefore, the big data from previously completed projects are gathered.

We formed dataset by merging information of projects extracted from big data in one place. The projects are grouped into three sizes: small, medium, and large. The class boundaries of this study are organization specific. The selected organizations were categorized as small to medium-sized organizations of Islamabad, Pakistan. However, these boundaries could vary when dealing with any other environment.

Furthermore, at the data preparation phase, the consolidated dataset of software development organizations is formed containing a total of 38 projects. This in return makes a dataset of 3091 records which is taken as a training dataset. Thereafter, the formed dataset is used for clustering and training purposes. The actual and estimated effort of these projects is presented in Fig. 2.

We evaluated the performances of our architecture using ten projects (P29–P38). From industry, 47 experts are participated in this study. The project characteristics (referred to in Table 1) that we have used for clustering are project size, volume,

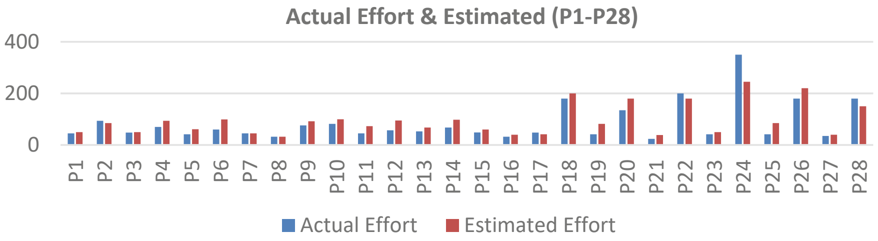


Fig. 2 Actual and estimated effort of projects used for training

Table 1 Variables used in this study

Variables/type	Categorical	Numeric
Item	Phase Activity Area Severity Completion	Item Size Priority Estimated effort Actual effort
Estimator	Role and their responsibilities Organizational competence Technical competence	Level Total experience Company experience Estimation experience
Project	Size Duration Turnover Complexity Development method	Actual effort Estimated effort Volume

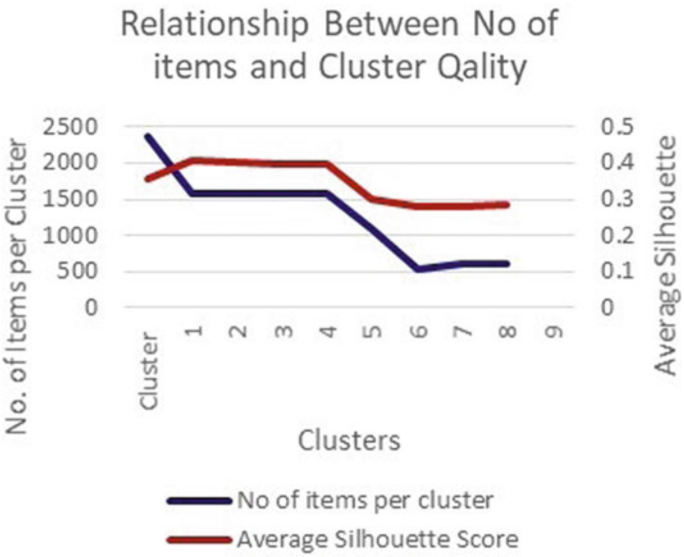


Fig. 3 Relationship of cluster quality and no. of items

complexity, and duration. The information is widely collected and stored for further usage.

After data preparation, first, we applied one best practice for effort estimation is known as project clustering [12]. By doing so, projects having the alike features are part of one cluster. The cluster formation of our dataset is presented in Fig. 3.

Then, we performed cluster analysis. In data mining, this is used to find the nature within a dataset as seen in work done by [13]. These project characteristics that are used to find a similar pattern is a volume, item actual effort, item-estimated effort, the actual, and estimated effort of the project along experience and priority. The red line displays the silhouette score assigned to molded clusters, while the blue line demonstrates no. of items per cluster. Moreover, we realized the decrease in numbers of the item increased in clusters and later for two values of K remain constant and afterward they tend to toward declination.

The exact silhouette scores of all formed clusters are calculated using the Orange tool. To build a model, there should be enough items. It is vital since the smaller dataset does not produce better-quality estimates. There are two criteria selected for this study. One of them is the silhouette score. The cluster having a value less than 0.302 is neglected. An alternative is the number of items present in each cluster.

Thus, at later stages, with the use of build architecture with machine learning algorithms that are used to provide effort estimates.

The formed cluster position is considered important as it is used for the architecture building phase. To estimate the effort of a new project, the architecture takes input from human experts. The information of new projects such as for estimated effort and turnover, actual and estimated effort of an item is removed from datasets. Later, these results are provided to human estimators to support their decision-making process for allocation of effort with lesser error. This information is necessary for the successful completion of projects.

From analysis, we have nominated three classes small, medium, and large. If we total number of projects present in each class, we noted nine projects are classified as small, 13 projects as a medium, and six projects as large. We have put up ten projects P29–P38 for model validation.

This phase depends on the results of previous project clustering. As the project clusters are used here, the projects P29–P38 are used to validate the results. Furthermore, this position of project cluster is used in the model building phase.

Thereafter, the next phase in the proposed architecture is model building. To build the models, we specified features and target variables from the list of variables presented in Table 1. Thus, we have one target variable and 25 variables which are features of projects.

The first set to build a model in the "Orange" tool is to read the dataset. After specifying features and targets, we apply machine learning algorithms such as k-nearest neighbor (KNN), random forest (RF), elastic net regression (E net Reg), support vector machine (SVM), and neural network (NN). First, the model is trained on the dataset and then evaluated using ten projects. Then, we compared the model, and the result of the comparison is presented in the next section. Eventually, we tested these models for effort estimation for "new projects." The next section provides an explanation of estimation for new projects.

3 Result

After the effort modeling and estimation phase, ten projects are tested for an optimum number of clusters, i.e., $K = \{3, 5, 7\}$. Moreover, we selected the models for each project to analyze which model is suitable for projects of the same size. To analyze deviations from in estimations, we picked absolute error, mean absolute error (AE), mean absolute error (MAE), prediction (Pred (0.25)), magnitude of mean relative error (MMRE), mean squared error (MSE), and root mean squared error (RMSE). Similar approaches are presented in studies [10] and previously by [14, 15].

The results show that the estimates which were made by the machine learning algorithm are near to actual. With the comparison of error magnitude for effort estimates between experts and models, better results are noted. We performed the abovementioned evaluation measures to validate results [2, 16–18].

When we applied machine learning, we noted the accuracy of random forest (RF) and support vector machine (SVM) is 70. After these techniques, elastic net regression is seen as the second-best option having a prediction accuracy of 60. In the intervening time, we also distinguished the prediction accuracy of k-nearest neighbor as 50. However, neural network performs worst. The prediction accuracy of the neural network is calculated as 40 when we formed three clusters, i.e., K = 3.

Table 2 Models outperformed for each project

Cluster	$K = 3$	$K = 5$	$K = 7$
Project	Model	Model	Model
P29	SVM	LR	SVM
P30	LR	LR	LR
P31	SVM	SVM	SVM
P32	SVM	SVM	SVM/KNN
P33	KNN	KNN	KNN
P34	SVM	SVM	SVM
P35	LR	LR	LR
P36	KNN	KNN	KNN
P37	LR	LR	LR
P38	KNN	KNN	KNN

The most suitable cluster according to the properties of the dataset is $K = \{3, 5, 7\}$. However, these values could change with different datasets and with the increment of projects in a pool. We noted a change in accuracy for the estimation model. When comparing the prediction accuracy of the support vector machine, we have seen the reduction inaccuracy of the model for $K = 3$ and 5 with a prediction accuracy of 50. However, when dividing the clusters to 7, the prediction accuracy increases to 70. Therefore, we can conclude support vector machine can be utilized for prediction. Furthermore, out of all results evaluation, we concluded support vector machine (SVM), linear regression (LR) with elastic net regression, and k-nearest neighbor (KNN) performed better than all other algorithms. Moreover, the algorithms which outperformed for different values of K are presented in Table 2.

However, if we keep on adding, more completed projects to the dataset and neighboring projects in the cluster would increase. As a result, the prediction accuracy of models with machine learning and clustering would increase has been provided in the work of Karna [10]. We have seen that the actual effort for 28 projects that were used for the training model was 2356[h] while the predicted effort was 2677[h]. Based on the actual and estimated effort that we were provided by the estimators after completing projects, we noted a difference on -321[h] or -13.32%.

Altogether 38 projects were selected in this study. Out of which, 28 projects (P1–P28) are taken for training models. We analyzed two projects that have no error; a margin of 10% was calculated for two projects. Furthermore, 20 projects were overestimated, and three were marked as underestimated projects. This shows experts are inclined toward overestimation the projects with relatively exceeding margins.

With all the previous discussions, we have provided validity of the research. The practical validation is provided by selected software development organizations. Generally, we noted that applying machine learning techniques with data mining improves effort estimation as compared to the estimates of humans.

Setting up overall conclusions in an identical environment is a challenging task. Primarily, because the procedure depends on the appropriate variables so the variables that were used in this study are same as variables found in work done by [10]. However, if the work done in the study could be conducted for other environments of software development organizations, this would, therefore, help in generalizing results. Another limitation of this study would be the use of this research work is the data used are collected from two organizations of similar environments. In the same context, we would want to collect data from more organizations, but here, this wasn't possible due to unwillingness in giving out the organizational data. Unfortunately, no similar work has been done before in this context and region. Additionally, this research was conducted on real data, which contributes to the value of this research. Moreover, if the proposed technique is adopted by more organizations, it would help them to get accurate effort estimates.

4 Conclusions and Future Work

Software development effort estimation is a necessary process to complete projects successfully. Therefore, we collected industrial big data of software projects and proposed software architecture for effort estimation. The proposed architecture consists of steps from data collection to application of machine learning and data mining algorithms and effort prediction. In the end, we also compared the results of the proposed architecture with other methods. From the comparison presented in this study, we concluded the combination of machine learning and data mining methods improve the accuracy of estimation when compared to humans. However, in the future, we intend to increase this work by making use of different clustering strategies and learners on similar and increased dataset to generalize results.

References

1. Pani SK, Mishra AK (2020) "Machine learning applications in software engineering: recent advances and future research directions." Int J Eng Res Technol 8(1):1–4. [Online]. Available: www.ijert.org
2. Ali A, Gravino C (2019) A systematic literature review of software effort prediction using machine learning methods. J. Softw. Evol. Process 31(10):1–25. https://doi.org/10.1002/smr.2211
3. Tanveer B, Vollmer AM, Braun S, Bin Ali N (2019) An evaluation of effort estimation supported by change impact analysis in agile software development. J Softw Evol Process 31(5):1–17. https://doi.org/10.1002/smr.2165
4. E. 1 B. B. H. L. Menzies Williams, Madachy "No title." Softw Process Improv Pract 14(November). https://doi.org/10.1002/spip.414
5. Jørgensen M (2004) A review of studies on expert estimation of software development effort. J Syst Softw 70(1–2):37–60. https://doi.org/10.1016/S0164-1212(02)00156-5
6. Nathanael EH, Hendradjaya B, Danar Sunindyo W (2015) "Study of algorithmic method and model for effort estimation in big data software development case study: geodatabase."

Proceedings—5th international conference electrical engineering informatics bridge knowledge between academy industrial community, ICEEI 2015, pp 427–432. https://doi.org/10.1109/ICEEI.2015.7352539

7. Divesh S (2017) Proceedings of the VLDB endowment. Proc VLDB Endow 10:2032–2033. https://doi.org/10.14778/3055540
8. Azzeh M, Nassif AB (2015) “Analogy-based effort estimation: a new method to discover set of analogies from dataset characteristics.” March 2014. https://doi.org/10.1049/iet-sen.2013.0165
9. Minku LL, Yao X (2017) Which models of the past are relevant to the present? a software effort estimation approach to exploiting useful past models. Autom Softw Eng 24(3):499–542. https://doi.org/10.1007/s10515-016-0209-7
10. Karna H, Vicković L, Gotovac S (2019) Application of data mining methods for effort estimation of software projects. Softw Pract Exp 49(2):171–191. https://doi.org/10.1002/spe.2651
11. Pandey P, Litoriya R (2020) Fuzzy cognitive mapping analysis to recommend machine learning-based effort estimation technique for web applications. Int J Fuzzy Syst 22(4):1212–1223. https://doi.org/10.1007/s40815-020-00815-y
12. Suresh Kumar P, Behera HS (2020) Estimating software effort using neural network: an experimental investigation, vol 1120. Springer Singapore
13. Ji J, Pang W, Li Z, He F, Feng G, Zhao X (2020) Clustering mixed numeric and categorical data with cuckoo search. IEEE Access 8:30988–31003. https://doi.org/10.1109/ACCESS.2020.2973216
14. Fadhil AA, Alsarraj RGH, Altaie AM (2020) Software cost estimation based on dolphin algorithm. IEEE Access 8:75279–75287. https://doi.org/10.1109/ACCESS.2020.2988867
15. Baghe A, Rathod M, Singh P “Software effort estimation using parameter tuned models”
16. Tariq S, Usman M, Fong ACM (2020) “Selecting best predictors from large software repositories for highly accurate software effort estimation.” J Softw Evol Process April:1–19. https://doi.org/10.1002/smr.2271
17. Azzeh M, Nassif AB (2018) Project productivity evaluation in early software effort estimation. J Softw Evol Process 30(12):1–12. https://doi.org/10.1002/smr.2110
18. Rak K, Car Ž, Lovrek I (2019) Effort estimation model for software development projects based on use case reuse. J Softw Evol Process 31(2):1–17. https://doi.org/10.1002/smr.2119

Scientific Music Therapy Technologies for Psychological Care and Rehabilitation in the COVID-19 Pandemic

Sergey V. Shushardzhan, Natalya Eremina, Ruben Shushardzhan, Tatiana Allik, and Kumyszhan Mukasheva

Abstract This article analyzes the complex challenges of the pandemic and prospects of the scientific music therapy technologies used in psychological care and rehabilitation patients with COVID-19. First, the researchers found that COVID-19 can occur in asymptomatic or mild clinical forms and severe clinical forms with the development of pneumonia and respiratory failure. More recently, another severe problem of the pandemic has appeared, and it is different mental disorders. The achievements of scientific music therapy are so significant that they improve mood and optimize the function of vital systems, even online, which is very actual for patients with COVID-19. That was the reason to present the basics and technologies of SMT, including the concept model of the multifunctional autonomous robot "Helper" for medical services, rehabilitation, and music therapy. The article's conclusive idea is that integration of science, advanced technologies, and art will play an increasingly significant role in modern rehabilitation treatment and hospital services in pandemics.

Keywords Pandemic COVID-19 · Scientific music therapy · Rehabilitation

1 Introduction

The pandemic outbreak of coronavirus disease in 2019 and its rapid spread around the world became the reason that COVID-19 was included in a number of the most current problems of our time. According to the Web portal "Coronavirus Today," on

S. V. Shushardzhan (✉) · N. Eremina · R. Shushardzhan
Academy of Rehabilitation Medicine, Clinical Psychology, and Music Therapy LLC, Moscow 143041, Russia
e-mail: medart777@yandex.ru

T. Allik
Doctor Music From Estonia" OÜ, 30322 Kohtla-Järve, Estonia

K. Mukasheva
Toraigyrov University, Pavlodar 140000, Kazakhstan

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_55

November 5, 2021, 249,521,825 people were infected with coronavirus in the world; the death toll is 5,048,630 [1], recovered 225,963,465 people.

The coronavirus infection COVID-19 is an acute respiratory disease caused by the new coronavirus (SARS-CoV-2). It is associated with increased mortality among people over 60 and persons with cardiovascular diseases, chronic respiratory diseases, diabetes, and cancer [2].

The coronavirus infection can attack the nervous system and other vital organs, but the most common clinical form is bilateral pneumonia [3].

COVID-19 can occur both in asymptomatic and mild clinical forms (80%) and in severe clinical conditions (20%) with the development of community-acquired pneumonia and respiratory failure. Another serious problem of the pandemic that has appeared is mental disorders.

A large part of patients with COVID-19 feel increased anxiety and fears from pulmonary insufficiency and numerous complications.

In that case, SMT, which has a relatively wide range of methods and advanced technologies, can play an essential role in providing mass psychological support and medical rehabilitation at all stages of patients with COVID-19 [4–6].

2 SMT Theoretical Basement

2.1 From the History of Music Therapy

The therapeutic use of music has a long history. Hippocrates, Aristotle, and other ancient sages a thousand years ago tried to treat with music nervous and mental patients. There are a lot of documentary mentions. They refer to different periods and civilizations and clearly show that doctors used music in medicine empirically. People used myths, metaphysical theories, or religious views in the explanations of therapeutic effects.

The twentieth century saw the spread of music therapy in different countries. In the United States, it was recognized after the Second World War. Music was one of the most effective tools for treating emotional disorders among war veterans. In addition, nowadays, more than 100 universities and colleges worldwide offer different educational programs.

2.2 Features of Scientific Music Therapy (SMT)

SMT is the new interdisciplinary direction of music therapy based on the synthesis of medicine, physics, arts, and modern technologies. The 1st author of this article developed the fundamentals of SMT in the early nineties of the last century in Russia, where he did researches on SMT in the Scientific Research Centre for Music Therapy and Healthcare Technologies (SRC MT HT) in Moscow.

In 2019, The European Union issued a special grant to an international group of specialists from Russia, Slovakia, Great Britain, Estonia, and the Czech Republic: "Comprehensive multi-professional approach to treating the patients using the elements of the scientific music therapy." That was the new international confirmation of SMT importance, based on Russian technologies, 11 patents, and some know-how (see, for example, patents [7–12].

Researches of the SRC MT HT identified in clinical studies various therapeutic effects of music therapy: psychotherapeutic, analgesic, hypotensive, etc. [13–17].

2.3 Regarding Musical-Acoustic Algorithms for Regulation of Vital Functions and Psychotherapy

SMT has a preference to study the features of complex body reactions—psychological, physiological, and bio-physical—to music by various modern diagnostic technologies.

This research has discovered three main musical-acoustic algorithms (S—sedative, T—tonic, and HR—harmonizing), which differ in frequency, amplitude, and intensity of sound, impacting specific musical characteristics.

In experiments (1996–2020), different algorithms of direct musical-acoustic impacts significantly change the vital activity of cells cultured in vitro: in some cases, activate, in others, inhibit [18].

Moreover, each algorithm causes characteristic changes in the nervous system and the level of hormones in the blood.

Experimentally, we revealed some following regularities.

1. S-algorithms inhibit the activity of the cerebral cortex, which causes mental and muscle relaxation, slows down the heart rate, and lowers blood pressure. S-algorithms reduce an elevated blood level of adrenaline, noradrenaline, and cortisol.
2. T-algorithms act in precisely the opposite way.
3. HR algorithms bring the nervous and hormonal systems into a state of equilibrium and stability, which positively influences the body, including the anti-aging effect.

Using found algorithms in digital music therapy programs is the key to psychotherapy and hormonal-level optimizing, which is essential for organism regulation and health improvement.

3 SMT Methods and Technologies

Thanks to the multi-method research of music's influence on the body, our team could develop more than 50 methods and innovative technologies.

There are three main directions:

(a) Active ones, where the patient himself takes part in it directly, for example, singing, or learning to play the elementary musical instruments;
(b) Receptive methods, where the patient passively receives the music therapy sessions (listening of live music playing or recorded playlists);
(c) High tech methods which use digital technologies and artificial intelligence are marked separately [18].

3.1 Vocal Therapy

Considering that the main target organ of the coronavirus is the lungs, doctors recommend using various types of breathing exercises in the rehabilitation of the patients.

At the same time, there is a well-known active music therapy method called in 1993 by the author, Shushardzhan S.V. "the Vocal Therapy." Vocal therapy aims to improve the respiratory system and the body's defenses by vibroacoustic stimulation of vital organs, optimizing higher nervous activity. It uses the principles of classical singing with a voice training system.

The systemic use of vocal therapy causes marked positive dynamics of indicators of lung capacity and also positively gets into the psycho-emotional state and the memory of patients.

The curative and healing effects of vocal therapy should be best suited to address many of the pressing problems of the convalescence period of COVID-19 patients, especially in the 60 + patient category at risk.

3.2 Digital Music Psychotherapy

We have developed some digital computer programs based on regulator algorithms and use them for stress, neurosis, insomnia, psychosomatic disorders, and life quality decrease in the condition of the monotonous atmosphere. The sessions of digital music psychotherapy must be in specially equipped patient rooms where the patients listen to treatment programs for 20–30 min. Any computer system with speakers or headphones is enough for it.

The doctors of any specialties, nurses, psychologists, etc., even without special training, can successfully use music therapy in treatment, prophylactic, and rehabilitation work, and they also can do it online.

3.3 Virtual Music-Art Therapy (VMART)

VMART is innovative psychotherapy and personality development method. We developed audio–visual digital computer programs for it with the world's masterpieces of painting and musical art.

Remarkable landscapes, forests, fields, high seas, medieval castles, colorful characters, sunsets and sunrises, seasons, all these picturesque creations as if come to life against the background of brilliant music.

Clinical research in different age groups has shown that if VMARTT for people who suffer from emotional liability and increased anxiety, in 84% of the cases, the neurotic symptoms fade away. The emotional state stabilizes, which was objectively confirmed by psycho-diagnostic tests of Luscher, Taylor, and example, 88% of the primary group patients noticed the aesthetic pleasure of watching virtual music-art therapy programs and an increased interest in musical art and painting.

Thanks to digital performance, practical, and easy-to-use virtual music-art therapy programs can be transmitted online to smartphones, personal computers, and televisions. That should be very important to use in COVID-19 hospitals and rehabilitation centers.

3.4 Meso-Forte Therapy

Meso-Forte therapy is an innovative patented high tech method for stress control and neurological rehabilitation, with anti-aging effects using acoustic algorithms-regulators [8, 10].

The steps of the Meso-Forte therapy procedure are the following:

(a) A moist mask soaked in reparative substances is applied on the human face;
(b) Mask-converter is superimposed;
(c) Headphones are put on top;
(d) Special music programs start to sound and act via mask-converter and headphones simultaneously.

Required equipment: The «Meso-Forte» hardware and software system + the mask-converter of acoustic waves «Bonny-Grand» + «Meso-Forte» music therapy programs (see Fig. 1).

Specialists use Meso-Forte therapy to rehabilitate post-COVID-19 patients with stress, insomnia, psychosomatic disorders, and decreased vitality.

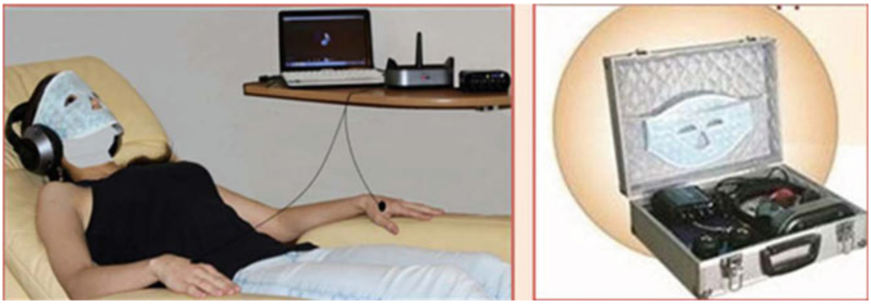


Fig. 1 Patented hardware–software complex "Bonny-Grand"

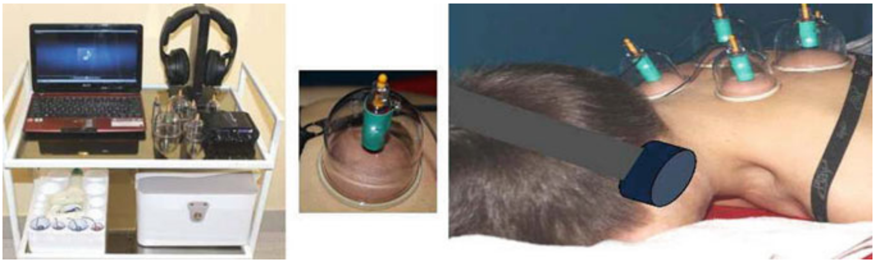


Fig. 2 Innovative hardware–software complex "Akutone" [9]

3.5 Akutone Therapy

Akutone therapy is the high tech method of pain-reducing and anti-stress therapy.

Required equipment: The "Akutone" hardware–software complex is capable provide receptive digital music therapy with simultaneous music therapy impact through special acoustic-magnetic-vacuum devices (see Fig. 2).

Acutone therapy is especially effective in disease treatment of joints, spine, muscles, and psychosomatic disorders.

3.6 The Autonomous Robot "Helper" for Rehabilitation, Music Therapy, and Medical Services

In 2019, together with partners from the Time of Robots LLC, we created an autonomous medical robot based on the R.Bot 100 Plus platform, known for its extensive work resource and high reliability.

A pilot sample could move along the specified routes, communicate, carry out biometric identification, and select health-improving music tracks (see Fig. 3) [19].

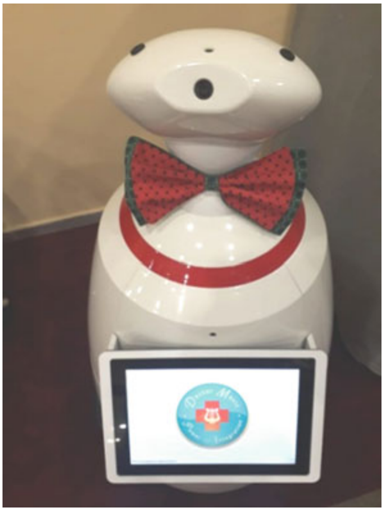


Fig. 3 Pilot sample of robot "Helper"

Currently, to the basic capabilities of the robot, called "Helper," we have added four functions that are critical in the face of a pandemic:

- *Disinfection of premises and robot self-disinfection.*
- *Drugs delivery.*
- *Telemedicine.*
- *Interactive* music therapy and virtual music-art therapy.

The helper robot has a male and female speech synthesizer, the ability to connect to interactive services. It can work both autonomously and under the control of a remote user/operator.

With a height of 105 cm robot weighs 45 kg, which is capable of operating from a rechargeable battery for up to 12 h, self-charging up to 5 h.

We developed music-acoustic psychotherapy programs in a digital format based on the advanced achievements of scientific music therapy, bioacoustics, and psychology, innovative psycho diagnostics. Robot's functionality has the corresponding software. Thanks to these programs, the robot asks questions, analyzes the answers received, and, on their basis, accurately selects therapeutic music tracks suitable for a particular patient.

Researchers found that their use effectively relieves stress and various psychosomatic disorders [19].

At the same time, these methods of psychological relief have a positive effect both in working with patients and with medical staff.

What do we expect in the systematic implementation of autonomous multifunctional robots of our concept in medical and rehabilitation practice?

- Significant reduction in nosocomial infection.
- Improvement of the epidemiological situation.

- Reducing workload on the medical staff.
- Expanding the range of medical rehabilitation services provided.
- Improving the psychological state of patients and quality of life.
- Increasing the efficiency of the work of a medical institution.

3.7 Regarding SMT Training

SMT technologies are easy to use but require some skills and competencies. That is why professional training in scientific music therapy began.

There are postgraduate higher courses in music therapy. Training is going with the participation of the European Academy of Music Therapy. Diplomas issued upon completion have official recognition in the European Union.

Scientific music therapists have a clear idea of the algorithmic mechanisms of music influence on a person, know-how to carry out the necessary diagnostics, and choose the best method or technology needed in each specific case.

4 SMT in the Rehabilitation of Patients with COVID-19: Preliminary Clinical Results and Discussion

According to the literature data, the main goal of rehabilitation in patients with COVID-19 is the restoration of the respiratory system and respiratory function and the removal of anxiety-depressive states, restoration of disordered functions, and improving the life quality [20].

Specialists have to use active, receptive, and high tech methods in the rehabilitation process, depending on the specific tasks. At the beginning of 2021, we started the rehabilitation program for patients after COVID-19.

We analyzed the rehabilitation results of 52 patients using scientific music therapy methods and technologies, and that was our first experience.

That patients, males and females of different ages had various problems after COVID-19: residual respiratory disorders (69.2%), mental disorders (59.6%), and separate somatic syndromes (30.7%).

We have the precedence to digital music psychotherapy, with vocal therapy, or a combination of the virtual music-art therapy with vocal therapy (10–15 sessions on each method). In some cases, in the presence of appropriate symptoms, Meso-Forte and Acutone therapy were used. See the rehabilitation results in Table 1.

SMT methods and technologies gave a positive result in the rehabilitation of the patients after COVID-19.

Respiratory disorders reduced—by 36.5%, mental disorders (depression, anxiety, insomnia)—by 40.4%, somatic syndromes—by 21.1%.

Our first experience with patient rehabilitation after COVID-19 showed encouraging results. Combination of vocal therapy with digital music psychotherapy or

Table 1 Results of rehabilitation after COVID-19 patients by SMT technologies

Health problems	Number (%) of patients before SMT	Number (%) of patients after SMT
Respiratory disorders	36 (69.2%)	17 (32.7%)
Mental disorders	31 (59.6%)	10 (19.2%)
Somatic syndromes	16 (30.7%)	5 (9.6%)

virtual music-art therapy improves respiratory function and emotional status. In addition, Meso-Forte and Acutone therapy help to treat somatic disorders.

Wherein, music therapy methods are popular among the patients who visit rehabilitation sessions with pleasure.

5 Conclusion

Scientific music therapy has the necessary theoretical base with a wide range of methods and technologies that make it possible to use them successfully in the rehabilitation of patients after COVID-19.

As shown by clinical observations, music therapy methods are well tolerated and have virtually no complications.

We did not use robotics in rehabilitation yet because this is a perspective project in the stage of development. But, we believe that the integration of science, technology, and art is the future of robotics. Such an innovative approach opens up new opportunities in medical service and rehabilitation.

We should not forget that during a pandemic, not only infected patients suffer. In addition, due to quarantine measures, hundreds of millions of people were involved in a stressful situation caused by fears, forced isolation, and economic problems.

It becomes clear that it is necessary to improve the system of global psychological assistance to the population. Here, we cannot be without creating powerful Internet portals with music therapy and psychological services.

Innovative technologies of scientific music therapy, integrated with artificial intelligence and telemedicine capabilities, must play an increasingly important role in the process of modern rehabilitation treatment and hospital services, which become especially great during a pandemic control and liquidation of its consequences.

References

1. Coronavirus today. https://koronavirustoday.ru/info/koronavirus-tablicza-po-stranam-mira-na-segodnya/
2. "Epidemiology and Prevention of COVID-19". Guidelines MP 3.1.0170–20 (in edition MP 3.1.0175–20 "Changes № 1 in MP 3.1.0170–20 "Epidemiology and Prevention of COVID-19", approved by Federal Service for Surveillance on Consumer Rights Protection and Human Welfare 30.04.2020")
3. Temporary guidelines "Prevention, diagnosis, and treatment of new coronavirus infection" (COVID-19). Version 6 (28.04.2020)" (approved by Ministry of Health of Russia) pp 1–18. https://static1.rosminzdrav.ru/system/attachments/ attaches/000/050/122/original/28042020_%D0%9CR_COVID-19_v6.pdf
4. Burkhart Chr. Music therapy providing some calm during COVID-19 Published: 27 Aug 2020, at 3:41 PM GMT+3. https://www.abc12.com/2020/08/27/music-therapy-providing-some-calm-during-covid-19/
5. Giordano F, Scarlata E, Baroni M, Gentile E, Puntillo F, Brienza N, Gesualdo L (2020) Receptive music therapy to reduce stress and improve wellbeing in Italian clinical staff involved in COVID-19 pandemic: a preliminary study. The Arts in Psychotherapy. 2020, 70, September 2020, 101688/Received 16 June 2020, Revised 8 July 2020, Accepted 11 July 2020, Available online 15 July 2020. https://doi.org/10.1016/j.aip, p 101688
6. Mastnak W Psychopathological problems related to the COVID-19 pandemic and possible prevention with music therapy. First published: 12 May 2020. URL: https://doi.org/10.1111/apa.15346
7. Shushardzhan SV (2011) The method of healing and rejuvenation of the skin. Patent number 2429026. Registered in the Russian State Register of Inventions
8. Shushardzhan SV (2013) Software and acoustic complex Profi-Grand. Patent number 126602. Registered in the State Register of Inventions of the Russian Federation
9. Shushardzhan SV, Shushardzhan RS (2013) Device for musical acoustic magnetic-vacuum effects on acupuncture points and reflexogenic zones Akuton. Patent number 129398. Registered in the State Register of Inventions of the Russian Federation
10. Shushardzhan SV (2013) Device for skin rejuvenation and recovery Bonnie Grand. Patent number 129820. Registered in the Russian State Register of Inventions
11. Shushardzhan SV (2014) The method of enhancing the growth of leukocyte mass and the complex correction of the blood in Vitro. Patent number 2518534. Registered in the State Register of Inventions of the Russian Federation
12. Shushardzhan SV (2014) The method of neuro-hormonal correction and rejuvenation with the help of musical-acoustic effects. Patent No. 2518538. Registered in the State Register of Inventions of the Russian Federation
13. Shushardzhan SV (2005) Music therapy guidance. Medicine 478
14. Shushardzhan SV, Shushardzhan RS, Eremina NI (2009) Substantiation of the reflex-resonance theory of acoustic influences and the prospects for the use of music therapy technologies. Bull Rehab Med 3(31):34–37
15. do Amaral MAS, Neto MG, de Queiroz JG, Martins-Filho PRS, Saquetto MB, Oliveira Carvalho VC (2016) Effect of music therapy on blood pressure of individuals with hypertension: a systematic review and meta-analysis. Int J Cardiol 214:461–4. https://doi.org/10.1016/P.-197
16. Mitrovic P, Stefanovic B, Paladin A, Radovanovic M, Radovanovic N, Rajic D, Matic G, Novakovic A, Mijic N, Vasiljevic Z (2015) The Music Therapy in hypertensive patients with acute myocardial infarction after previous coronary artery bypass surgery. J Hypertension 33:134
17. Zanini C, Sousa AL, Teixeira D, Jardim PC, Pereira D, Vilela B (2018) Music therapy as part of the treatment of hypertensive patients. J Hypertension 36:260

18. Shushardzhan S (2017) Scientific music therapy—achievements and prospects. In Slovakia, Šamorin, proceedings of the xxi interdisciplinary medical congress of natural medicine with international participation, p 17
19. Shushardzhan SV, Petoukhov SV (2020) Engineering in the scientific music therapy and acoustic biotechnologies. In: Hu Z, Petoukhov S, He M (eds) Advances in artificial systems for medicine and education III. AIMEE 2019. Advances in intelligent systems and computing. vol 1126, pp 273–282. Springer, Cham
20. Wang TJ, Chau B, Lui M, Lam GT, Lin N, Humbert S (2020 Sep) Physical medicine and rehabilitation and pulmonary rehabilitation for COVID-19. Am J Phys Med Rehabil 99(9):769–774. https://doi.org/10.1097/PHM

Analysis of the Development of Electrification of Urban Public Transport in China Based on Life Cycle Cost Theory

Qingdong Luo, Jingjing Lou, Xiyuan Wan, Yunhan Li, and Pengfei Zheng

Abstract Since 2009, under the vigorous promotion and drive of the country's active industrial development policy, China's public transport has evolved from a single traditional fuel public transport to natural gas, hybrid, electric, and hydrogen in just ten years. This paper takes these five types of public transport as the research object and uses the life cycle cost theory to analyzing their economy, the relevant actual operation data are collected by investigation and establishes the life cycle cost measurement model of the above five types of urban public transportation. The difference analysis is carried out on the initial purchase cost, use cost, maintenance cost, scrap income, and life cycle cost. On this basis, this paper analyzes the reasons from an economic perspective why China has chosen pure electric power as the development path of urban public transport in a variety of energy types after years of exploration.

Keywords Public transport · Life cycle cost · Economy · Cost comparison · Electrification

1 Introduction

In the transportation industry, public transport has been pioneers in the promotion of energy saving and new energy vehicles. Since 2009, China launched the "Ten Cities and Thousands" new energy vehicle demonstration project, then the "Energy Saving and New Energy Vehicle Industry Development Plan (2012–2020)" released in 2012, and the newly released "New Energy Vehicle Industry Development Plan (2021–2035)," under the vigorous promotion and drive of the country's active industrial development policy, and China's public transport has evolved from a single traditional fuel public transport to natural gas, hybrid, electric, and hydrogen in just ten years.

Q. Luo · J. Lou · X. Wan · Y. Li · P. Zheng (✉)
Yiwu Industrial & Commercial College, Yiwu 322000, China
e-mail: pfzheng@126.com

P. Zheng
East China University of Science and Technology, Shanghai 200237, China

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_56

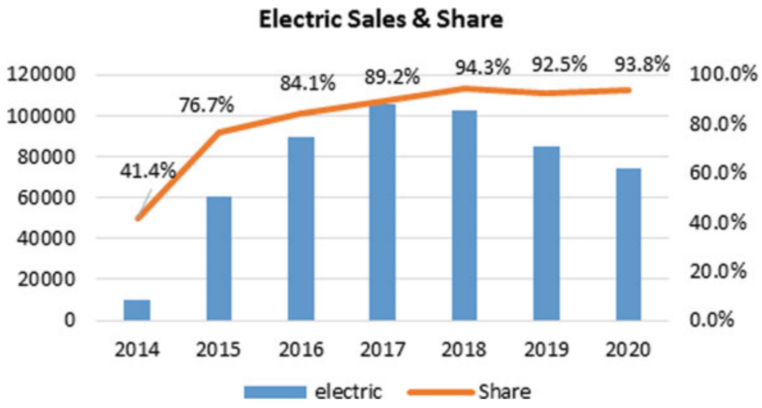


Fig. 1 Sales and share

Data from the China Association of Automobile Manufacturers show hybrid buses peaked at 17,000 units sold in FY 2015, then quickly fallen back to under 4,000 units sold in five years. Since the promotion of electric bus, sales have been rising year by year, reaching 102,523 units in 2018, accounting for 94.3% of all sales of new energy buses. Thereafter, the sales ratio in 2019 and 2020 is also above 92.5%, which is the absolute main force in the development of China's new energy bus industry [1–5]. The sales and share of electric buses in the last 7 years are shown in Fig. 1.

The vigorous development of new energy automobile industry, on the one hand, effectively alleviate the increasingly serious environmental and energy pressure, on the other hand, the automobile industry, an important pillar industry of the national economy, has ushered in new development opportunities. In this paper, takes the domestic 12-m bus with five types of fuel, natural gas, hybrid, electric, and hydrogen as the research object. Through field investigation, relevant actual operation data are collected, to establish the life cycle cost measurement model. By analyzing the differences in cost of initial purchase, cost of operational, cost of maintenance, cost of operational fault, and cost of disposal and total life cycle cost, this paper analyzes the reasons why China chooses electric as the development path of urban public transport after years of exploration from an economic perspective.

2 Theory Modeling

2.1 Data Collection

In order to ensure the authenticity, reliability, and comparability of the model data of public transportation, this paper uses field research to collect the driving and operation data of different energy types of public transportation in several provincial capitals. The data sample was selected from the leading bus manufacturer in China, and the actual operating data of five types of new energy public transports of the same 12-m model of the company: fuel, gas, hybrid, pure electric, and hydrogen energy. Through the relevant statistical analysis and data analysis of the collected sample data, the cost analysis data such as fuel cost in 100 km, maintenance cost, and maintenance cost of the actual operation of the five types of energy public transports are obtained.

2.2 Life Cycle Cost Theory Model

Mathematical model of engineering estimation method for life cycle cost analysis.

$$\begin{aligned} C = {} & C_m(C_{m1}, C_{m2}, C_{m3}, \ldots) + C_u(C_{u1}, C_{u2}, C_{u3}, \ldots) \\ & + C_f\big(C_{f1}, C_{f2}, C_{f3}, \ldots\big) + \cdots \end{aligned} \tag{1}$$

C_m, C_u, C_f is the unit cost of different stages, respectively.

Vehicle life cycle cost analysis is a means of evaluating the overall economics of a vehicle’s life cycle. By analyzing the characteristics of each stage of the life cycle of the five types of public transportations to be studied and ignoring some of the uncertainty cost factors, the life cycle cost measurement model established in this paper can be expressed in Eq. (2). The model consists of five modules: cost of initial purchase CI, cost of operational use CO, cost of maintenance CM, cost of operational fault CF, and cost of disposal CD.

$$\mathrm{LCC} = \mathrm{CI} + \mathrm{CO} + \mathrm{CM} + \mathrm{CF} - \mathrm{CD} \tag{2}$$

3 Life Cycle Cost Calculation and Difference Analysis

Considering the high complexity of a complete and comprehensive evaluation of the life cycle costs of public transportation, the large amount of data and the fact that some of the data are not easy to collect, and the differences in the variables used to evaluate the costs of different types of vehicles can make it difficult to conduct comparative analysis. This paper is based on the constructed life cycle cost model as an econometric model. Based on the constructed life cycle cost model as a measurement model, this paper has costed the life cycle of five types of public transportation and completed the economic evaluation of different energy types of urban public transportation through the comparative analysis of their life cycle cost differences.

3.1 Cost of Initial Purchase CI

The cost of initial purchase *CI* calculation formula is shown in (3). For fuel and gas buses, the CI is mainly composed of urban bus purchase cost CI_1 and vehicle purchase tax CI_2. For hybrid and electric buses, according to “the Notice on Exemption from Vehicle Purchase Tax for New Energy Vehicles” [6], the purchase tax is exempted, while the government purchase subsidy CI_3 is additionally deducted.

$$\mathrm{CI} = \mathrm{CI}_1 + \mathrm{CI}_2 - \mathrm{CI}_3 \tag{3}$$

where $\mathrm{CI}_1$is the purchase cost of the public transport; $\mathrm{CI}_2$is the vehicle purchase tax; CI_3 is the government purchase subsidy of the new energy public transport.

(1) The Vehicle Purchase Tax CI_2

The vehicle purchase tax CI_2 for fuel and gas buses is based on “the Interim Regulations of the People’s Republic of China on Vehicle Purchase Tax” [7], and the purchase tax to be paid is 10% of the purchase price of the public transport.

(2) Government purchase subsidies for new energy buses CI_3

According to the “Notice on Further Improving the Financial Subsidy Policy for the Promotion and Application of New Energy Vehicles” [8], hybrid, pure electric two kinds of public transports have government purchase subsidies CI_3.

According to the 2021 subsidy program, 12 m hybrid bus enjoys 34,200 yuan subsidy, 12 m electric bus enjoys 81,000 yuan subsidy. In addition, fuel cell public transports enjoy incentives for demonstration applications in urban clusters, and single vehicle purchases do not enjoy government purchase subsidies [9].

According to the above-related policies and cost analysis, the cost of initial purchase and comparison of the five energy types of public transportation is shown in Fig. 2.

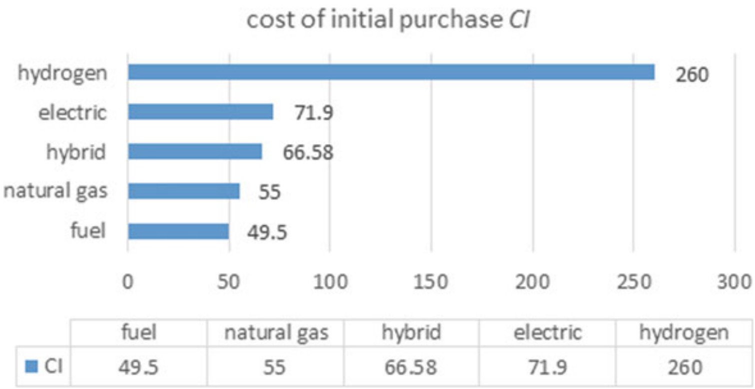
3.2 Cost of Operational CO

Cost of operational CO is mainly composed of bus operating fuel cost CO_1, for new energy buses need to additionally subtract the government operating subsidy CO_2.

(1) Fuel Cost CO_1

In this paper, the bus life cycle mileage, average 100 km energy consumption, and fuel price are used to calculate the fuel cost CO_1, as shown in Eq. (3):

$$\mathrm{CO}_1 = M \times S \times P \tag{3}$$



	fuel	natural gas	hybrid	electric	hydrogen
■ CI	49.5	55	66.58	71.9	260

Fig. 2 Cost

where *M* is the average 100 km energy consumption of public transport; S is the mileage of public transport life cycle P is the unit fuel price.

According to the research results and data analysis, the average annual mileage of the bus is 55,000 km, the service life is 8 years, and the total life cycle mileage is 440,000 km; the study assumes that the market price of fuel and the 100 km energy consumption of the five models remain constant during the life cycle, and based on the China Price Yearbook, the fuel price is obtained by fitting with the least squares method.

(2) The Government Operating Subsidy CO_2

According to the "notice of the three departments on improving the price subsidy policy for public transport refined oil to accelerate the popularization and application of new energy vehicles" [10], hybrid, electric, hydrogen three kinds of public transports to enjoy government purchase subsidies CO_2, the subsidy standards are shown in Table 1.

According to the above analysis, a list of the operating costs of five types of public transportation is shown in Table 2. After deducting the government operation subsidy, the life cycle operation cost comparison of the five types of public transportation is shown in Fig. 3

Table 1 The subsidy standards

Vehicle length L(m) Unit: 10,000 yuan / vehicle / year			
Types	$6 \leq L < 8$	$8 \leq L < 10$	$L \geq 10$
Electric	4	6	8
Hybrid	2	3	4
Hydrogen		6	

Table 2 List of the operating costs of five types of public transportation

Type	Total km	Fuel cost per 100 km Unit: CNY	Unit: CNY 10,000		
			CO_1	CO_2	CO
Fuel	440,000	241	106	/	**106**
Hybrid	440,000	180	79.2	32	**47.2**
Natural gas	440,000	210	92.4	/	**92.4**
Electric	440,000	94.5	41.6	64	**– 22.4**
Hydrogen	440,000	420	184.8	48	**136.8**

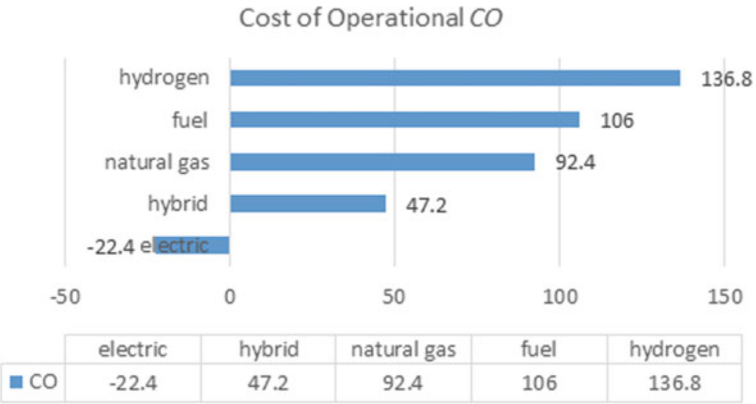


Fig. 3 The life cycle operation cost comparison

3.3 Cost of Maintenance CM, Cost of Operational Fault CF

Based on the statistical results of the operation and maintenance, primary maintenance, secondary maintenance, and overhaul cost data of the five types of public transport in the vehicle life cycle within 5 years, this paper mainly considers the material cost, not including the infrastructure investment cost and labor cost, and calculates the average annual cost to estimate the operation and maintenance cost CM + CF.

$$\mathrm{CM} + \mathrm{CF} = \sum_{5}^{i=1} (\mathrm{CM}_i + \mathrm{CF}_i) \tag{4}$$

where CM_i and CF_i are the maintenance and maintenance costs per year, respectively $i = 1, 2, \ldots, 5$.

According to the survey, the average annual maintenance and repair cost of fuel public transport are CNY 11,232; the average annual maintenance and repair cost of

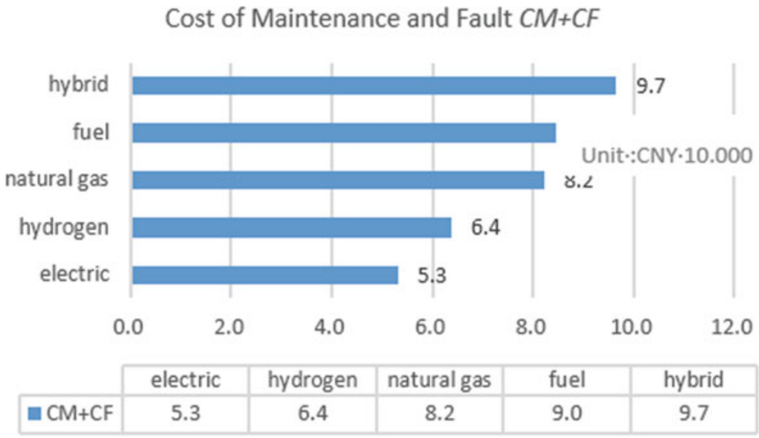


Fig. 4 Life cycle operational maintenance and repair costs

natural gas public transport are CNY 10,275; there is a small sample of hybrid bus holdings, with an average annual maintenance, and repair cost is CNY 12,075;

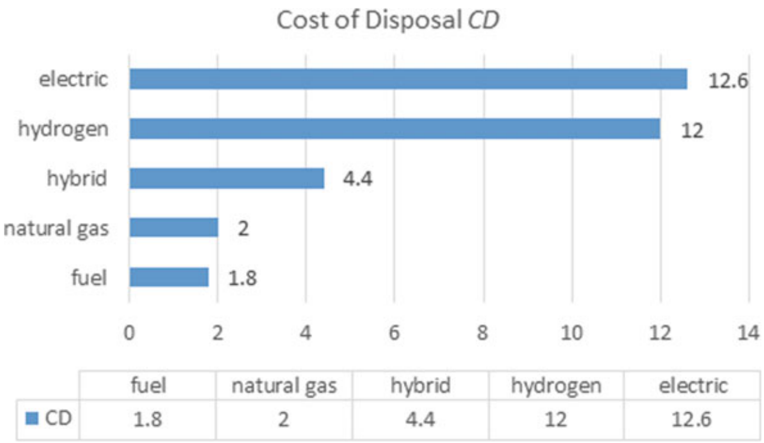
The maintenance of electric bus motor, battery, and electric drive system suppliers is more than 8 years, because the traditional engine, transmission, clutch, and other assembly parts are canceled, and the maintenance amount is greatly reduced. The average annual maintenance and repair cost are CNY 6637.

Hydrogen bus is still in the demonstration operation stage, without research data in this regard, an increase of 20 percent on an electric basis is estimated at an average annual maintenance and repair cost of CNY 7964 [11–14]. Life cycle operational maintenance and repair costs for five energy types of public transportation are shown in Fig. 4.

3.4 Cost of Disposal CD

In accordance with the "mandatory scrapping standards for motor vehicles" [15], owners are generally compensated for scrapping at 4% of the purchase cost, fuel bus scrap recycling income is CNY18,000, and gas bus scrap recycling income is CNY20,000. New energy bus scrap income consists of battery recycling income and vehicle recycling income (excluding batteries).

At present, the cycle life of lithium iron phosphate battery in electric bus can reach more than 3000 times. According to the calculation that the energy of the scrap battery in eight years decays to 70–80% of the original value, the price of the battery repurchase for the cascade utilization is about 30% of that of the new battery. The vehicle recycling revenues (excluding batteries) of electric, hybrid, and hydrogen were CNY 26,000, CNY 18,000, and CNY 102,000, respectively. Five types of public transportation scrap recycling income as shown in Fig. 5.

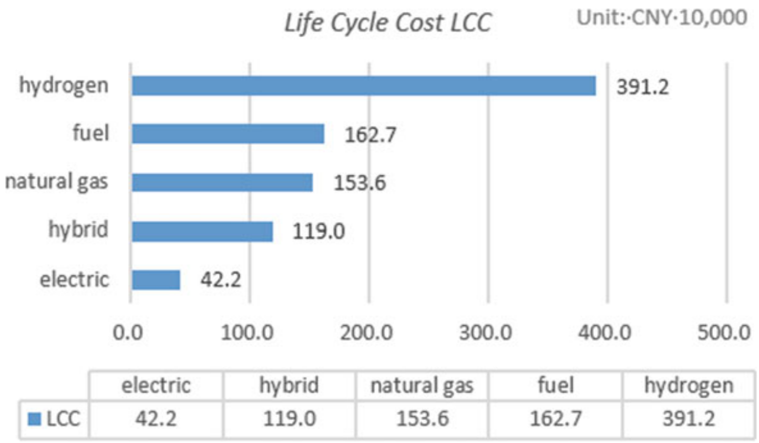


	fuel	natural gas	hybrid	hydrogen	electric
■ CD	1.8	2	4.4	12	12.6

Fig. 5 Scrap recycling income

3.5 Life Cycle Cost LCC

According to the above research and the life cycle formula, the life cycle costs of five types of public transportation are summarized in Fig. 6.



	electric	hybrid	natural gas	fuel	hydrogen
■ LCC	42.2	119.0	153.6	162.7	391.2

Fig. 6 LCC

3.6 Analysis of Research Results

According to the comparison of life cycle cost *LCC* of five types of public transportation and the comparison of life cycle cost *LCC1* after deducting government subsidies, this paper analyzes the differences of life cycle cost of five types of public transportation, the following conclusions are reached:

(1) Electric bus has the lowest life cycle cost which has obvious economic advantages. With the development and maturity of technologies related to the three electric systems of electric bus, electric buses in the *LCC* modules show obvious advantages, especially in the operational use cost *CO* module, with the development of core technologies related to the three electric systems of pure electric vehicles. Recently, the government-implemented energy saving and new energy bus operating subsidy standards CO_2 subsidy standards have already exceeded the public transport charging consumption. 8 years to produce a balance of CNY224000.

(2) As a demonstration of hydrogen fuel, the acquisition cost and operating cost of public transport are much higher than those of other four energy models. The manufacturing cost and fuel usage cost are higher. So it will take time for massing application.

4 Conclusion

This paper collects actual operation data of five energy types of urban buses based on the life cycle cost theory and establishes a life cycle cost measurement model for life cycle cost calculation and completes the economic evaluation of different energy types of urban buses by analyzing the life cycle cost differences. The following conclusions and perspectives are drawn:

(1) The results of the study show that electric buses have the lowest life cycle cost and obvious economic advantages while it meeting the needs of the national energy conservation and emission reduction Blue Sky Defense War. The development of electric bus is the result of both policy development and market demand.

(2) There have greater development advantages in the public service sector to implementation of electric bus. But the electric buses also have corresponding limitations. First, restricted by the charging time and the lagging supporting of charging facilities, this requires strong support from local governments to build more charging piles; Secondly, due to the restriction of battery endurance mileage, battery manufacturers need to upgrade their technology to increase the pack energy density of battery pack from 140–155 Wh/kg to > 175 Wh/kg.

(3) Although the hydrogen bus being demonstrated do not have a cost advantage in recently but when the life cycle costs of hydrogen bus fall to a cost comparable to or even lower than that of fuel bus, in another word, when the purchase

cost of hydrogen bus is reduced by 40% or the cost of hydrogen falls from the current CHY80 to less than CHY40 or lower. In that time, it will be the beginning of the mass application of hydrogen bus, and it is expected that by 2050, hydrogen fuel cell vehicles will become an important part of China's new energy system.

References

1. Li L (2020) The development path of comprehensive electrification of new energy bus industry. Autom Accessories, pp 33–37
2. Meng X, Gu A, Wu X, Liu B, He Z, Mao Z (2020) A look back at the hot spots of hydrogen energy policy, industry and technology development in China in 2019. Sci Technol Herald 38(3):172–183
3. Ren Y, Li H et al (2009)A consumer-based life-cycle cost model and analysis of electric vehicles.Techno-economic (11) 54–58
4. Tang B, Liu J (2013) Economic analysis of the development of pure electric and hybrid buses in China. China Energy 37–42
5. Wu K (2003) Development trend of low-emission vehicle technology. J Chang'an Univ (Nat Sci Ed) 67–70
6. Announcement of the four ministries on the exemption of vehicle purchase tax for new energy vehicles (Finance [2017] No. 172)
7. State Council of the People's Republic of China DecreeInterim Regulations of the People's Republic of China on Vehicle Purchase Tax No. 294
8. Notice on Further Improving the Financial Subsidy Policy for the Promotion and Application of New Energy Vehicles. Financial Construction [2020] No. 593
9. Notice on the Demonstration and Application of Fuel Cell Vehicles (Financial Construction [2020] No. 394)
10. Notice on improving the price subsidy policy for refined oil for urban buses to accelerate the promotion and application of new energy vehicles (Financial Construction [2015] No. 159)
11. Ahman VV, Nilsson M, Nilsson LJ (2018) Assessment of hydrogen direvt reduction for fossil-free steelmaking. J Cleaner Prod 203(1):736–745
12. Li J, Li G et al (2021) Overview of the progress and development prospects of key technologies for hydrogen production under the goal of carbon neutrality. Therm Power Gener 6:1–8
13. Li X, Yu B (2019) Peaking CO_2 emissions for China's urban passenger transport sector. Energy Policy133:110913
14. Abdalla AM, Hossain S, Nisfindy OB et al (2018) Hydrogen production, storage, transportation and key challenges with applications: a review. Energy Convers Manag 165:602–627
15. Ministry of Commerce, Development and Reform Commission et al (2013) The mandatory scrapping standards for motor vehicles, No. 12

A Systematized Literature Review: Internet of Things (IoT) in the Remote Monitoring of Diabetes

Belinda Mutunhu, Baldreck Chipangura, and Hossana Twinomurinzi

Abstract The Internet of Things (IoT) is an important emerging technology that enables (usually) pervasive ubiquitous devices to connect to the Internet. Medical and Healthcare Internet of Things (MHIoT) represents one of the application areas for IoT that has revolutionized the healthcare sector. In this study, a systematized literature review on the adoption of MHIoT for diabetes management is done to investigate the application of IoT in the monitoring of diabetes, key challenges, what has been done, in which context, and the research gap using Denyer and Transfield's systematic literature review methodology. The key findings reveal that developing nations are lagging despite the greater benefits of MHIoT in such resource-constrained contexts. The findings suggest that infrastructure costs, security, and privacy issues are most important in the adoption of MHIoT for diabetes management. The opportunities presented by MHIoT surpass the challenges as healthcare costs are reduced in a resource-constrained context. Further research in infrastructural needs and privacy concerns is needed to take full advantage of these benefits and address the challenges.

Keywords Health care · Developing countries · Developed countries · Sensors · Glucose · Blood sugar · Actuators · Remote health monitoring

1 Introduction

The Internet of Things is a method of connecting network-capable devices such as sensors and actuators to the Internet to extract usable data or information through standard Internet Protocol (IP)[1]. IoT-based medical acquisition detectors can be

B. Mutunhu (✉) · B. Chipangura
University of South Africa, UNISA, PO Box 392, Pretoria 0003, South Africa
e-mail: 69970777@mylife.unisa.ac.za

B. Chipangura
e-mail: ChipaB@unisa.ac.za

H. Twinomurinzi
University of Johannesburg, PO Box 524, Auckland Park 2006, South Africa
e-mail: hossanat@uj.ac.za

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_57

used to monitor the glucose level in diabetes. Diabetes is a chronic disease caused by an increase in the levels of glucose, which causes organ damage [2]. Diabetes has no cure, and constantly monitoring it is vital for prolonged healthy life. Africa is alleged to have the highest proportion of undiagnosed diabetes, with 60% of adults unaware of their condition [3]. Developing countries are still not fully aware of the benefits of IoT in the management of chronic diseases [4]. Low adoption rates are attributed to the high costs of technology adoption, lack of funding, lack of diabetologists, inadequate policy framework, security, and privacy concerns [5]. These challenges are not well researched and documented. There are other factors, such as culture, that have been shown to influence technology adoption, but there are limited studies linking culture to IoT adoption for diabetes. Researchers pose that this important detail lacks in existing models [6]. IoT presents an effective platform to monitor diabetes, providing health benefits as well as reducing the financial burden on patients in developing nations. It is with this background that the authors are conducting this research to bridge this technology gap.

2 Literature Review

Kelly [7] assessed IoT adoption and wearable devices in health care, and they note that IoT applications ought to be explored for different geographical settings with an emphasis on standardized protocols and interoperability as enablers may differ. Kim's [8] study on the Korean context identified service quality, trust, and risk perception as the main factors influencing the use and acceptance of IoT in healthcare service, while Zahedul [9] investigated the factors affecting the adoption of mHealth services in Bangladesh by the Unified Theory of Technology Acceptance and Use of Technology (UTAUT) model. Their findings reveal that variables such as perceived creditability, trust, awareness, and attitude must be taken into account when promoting the intention to adopt IoT technology. Costea-Marcu and Militaru's [10] study was explored through the lens of the technology acceptance model (TAM). Romanian consumers confirmed that the perceived usefulness, ease of use, confidence, and social influence and confidence as the most significant factor toward the acceptance of medical devices that are based on IoT technology and health monitoring. Yuan and Cheah [11] applied the diffusion of innovations (DOI) model and TAM to study the degree to which IoT is accepted by Malaysians. They emphasized that regulatory concerns, security, and infrastructural needs, and data privacy should be investigated before any adoption of IoT can take place. Tripathi and Pandit [12] developed a framework for the adoption of IoT in organizations from a systems dynamic perspective. Their study conforms with Brous [13] who also identified organizational, technological, and human factors as the key factors to be considered for successful IoT implementation. Roy [14] examined the adoption of IoT-based innovation by urban poor communities as they are the dominant source of urban IoT-based innovation. They identified factors influencing the adoption of IoT to be inadequate technology awareness, social acceptance, and consumer needs.

3 Methodology

Denyer and Tranfield [15] prescribed a systematic review protocol which this systematic review also adopted. Figure 1 shows a schematic representation of the adopted review protocol. The stages are as follows:

3.1 Question Formulation

In the planning phase, the review protocol and the review question were formulated from the aim of the systematic review which is to investigate opportunities, key challenges, theoretical frameworks used, in which context, and identify the research gap in IoT literature/research.

Research Question
In conducting this review, the following question was proposed to find answers from the review.

RQ1: What are the opportunities, key challenges, and research gaps in IoT Diabetes monitoring?

RQ2: What are the theoretical frameworks that have been adopted in IoT Diabetes monitoring?

3.2 Locating Studies

The construction of the search terms was derived from the review question and keywords. The following search string was formulated. ("Adoption") AND ("Internet

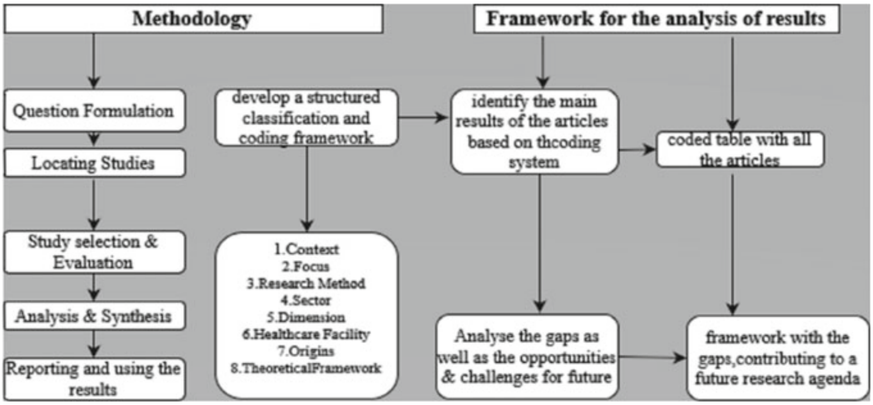

Methodology
Framework for the analysis of results
Question Formulation
Locating Studies
Study selection & Evaluation
Analysis & Synthesis
Reporting and using the results
develop a structured classification and coding framework
1.Context
2.Focus
3.Research Method
4.Sector
5.Dimension
6.Healthcare Facility
7.Origins
8.TheoreticalFramework
identify the main results of the articles based on thcoding system
coded table with all the articles
Analyse the gaps as well as the opportunities & challenges for future
framework with the gaps,contributing to a future research agenda

Fig. 1 Systematic literature review process and results framework for the study [15]

of Things” OR “IoT”) AND (“Diabetes*” OR “blood glucose” OR “blood sugar”) OR (“remote monitoring” OR “monitor*”). These search strings were then applied to search four databases (IEEE Xplore, ScienceDirect, Scopus, Web of Science). These databases were selected because they cover the key topics addressed in this paper and are generally used in recent IoT research [13].

3.3 Study Selection and Evaluation

For the initial search, only 457 papers from the 4 databases were identified. The inclusion criteria were based on: (1) articles published between January 2015 to present; (2) studies published in English; (3) research from peer-reviewed journals and conferences; (4) articles that mention IoT in diabetes within their title or content; (5) papers must be in a full or short version (not abstracts). After this initial search, duplicates were removed and 360 were left. To reduce the number of papers from the initial search, the titles and abstracts of the remaining papers were screened against the following exclusion criteria: Articles that do not solely focus on IoT in diabetes monitoring, articles focusing on chronic diseases and not exclusively diabetes, articles that do not focus on IoT use in diabetes from a health and technological perspective. After the above exclusion criteria, only 169 papers were left. The full-text analysis was done, and only the publications able to contribute to answering the review were selected. After this final screening, only 21 papers were identified as relevant to this research.

3.4 Coding and Classification

After amassing and screening the relevant studies, a modified classification framework was constructed consisting of letters and numbers to classify and code the articles [16]. Table 1 depicts the classification framework and codes.

4 Analysis and Synthesis

After analyzing the articles, twenty-one (21) studies were selected to be classified and coded using a classification framework adopted from [16] (Table 2).

Table 1 Classification and coding framework

Classification	Description	Codes
1. Context	Developed countries	1A
	Developing countries	1B
	Not applicable	1C
2. Focus	IoT in the monitoring of diabetes as the main theme	2A
	IoT monitoring of diabetes as supporting theme	2B
	IoT as the main theme	2C
3. Research methodology	Qualitative	3A
	Quantitative	3B
	Mixed methods	3C
	Survey	3D
4. Dimensions	Adoption/monitoring	4A
	Activity and diet tracking	4B
	Opportunities and challenges	4C
5. Healthcare facility (HCF)	Hospital	5A
	Home	5B
	Rehabilitation center and old people's home	5C
	Not mentioned	5D
6. Origin (continents)	America	6A
	Europe	6B
	Asia	6C
	Oceania	6D
	Africa	6E
	Not applicable	6F
7. Theoretical framework	TAM	7A
	UTAUT	7B
	DOI	7C
	Combination of models	7D
	Not mentioned	7E

4.1 Context and Origin

Ten articles focused on developed countries (1A) in comparison to developing countries (1B)**.** Thirteen research studies about remote monitoring of diabetes originated from Asia (6C). No study originated from the African (6E) continent. The findings suggest that there is a research opportunity for IoT diabetes management in resource-constrained contexts specifically Africa since the context is unique and infrastructure is not as developed, yet the incidence of diabetes is on the increase [17].

Table 2 Results of the codification framework

Authors	Context	Focus	Method	Sector	Dimensions	HCF	Origins	Framework
Roy et al. [14]	1B	2C	3C 3D	4B	5A	6D	7C	8E
Rodbard [21]	1A	2A	3D	4A	5B 5D	6D	7A	8E
Deshkar and Menon (2016)	1A	2A	3D	4A	5D	6D	7C	8E
Hsu and Lin [31]	1A	2B	3A	4C	5A 5D	6D	7C	8F
Costea-Marcu and Militaru [10]	1B	2B	3D	4A	5D	6A	7B	8A
Mishra [28]	1B	2A	3D	4A	5D	6D	7C	8F
Kao et al. [34]	1B	2C	3D	4C	5A 5D	6D	7C	8A 8B
Longva and Haddara [24]	1C	2A	3D	4C	5D	6D	7C	8E
Yuan and Cheah [11]	1A	2C	3B 3D	4A	5A	6D	7C	8A 8C
Kato et al. (2020)	1A	2A	3B	4C	5C	6D	7C	8E
Alkhudairi [35]	1B	2A	3C	4A	5A	6B	7C	8B
Qiu et al. (2018)	1A	2C	3A	4C	5D	6B	7C	8E
Lee and Lee (2018)	1A	2B	3B 3D	4C	5A	6D	7C	8D
Ahmadi et al. (2019)	1C	2C	3D	4A	5D	6 B	7B	8E
Tripathi [1]	1C	2C	3D	4B	5D	6D	7F	8E
Canhoto and Arp [32]	1A	2C	3A	4A	5A	6D	7B	8D
Kang et al. (2019)	1B	2C	3B 3D	4A	5A 5D	6A	7C	8E
Hanley et al. (2015)	1A	2A	3A	4A	5 B	6C	7B	8E
Mital et al. [33]	1B	2C	3B	4 C	5A	6D	7C	8D
Baker et al. (2017)	1C	2C	3D	4A	5D	6A	7F	8E
Brazionis et al. (2017)	1A	2A	3D	4A	5 B	6A	7D	8E

4.2 Focus

The articles that focused their research extensively on diabetes and no other diseases were classified as (2A) and were eight. Articles that used it as a supporting theme, i.e., merely mentioned diabetes and other diseases (three) were classified as (2B), while studies that focused mainly on IoT as (2C) were ten. Few works have used IoT in the remote monitoring of diabetes as the main theme. There is a need to contextualize IoT applications to country-specific problems and tactical ingenuities. For example, the USA is leading in healthcare IoT and in leveraging health-related data from IoT devices [18]. In Zimbabwe, an IoT intervention has the potential to promote ubiquitous access to health care thereby serving as a viable solution to alleviate the healthcare crisis in the remote monitoring of diabetes [19].

4.3 Research Methodology

Ten articles utilized surveys (3D) as research methods. Four studies utilized qualitative methodology (3A), while five studies utilized quantitative methodologies (3B) as part of their studies. Two studies (3C) utilized the mixed methodology approach. Four studies that focused on the remote monitoring of diabetes as their main theme (2A) utilized either qualitative or quantitative methodology as their preferred methodology, while those studies that focused on IoT as their main theme (2C) utilized surveys (3D).

4.4 Dimensions

Seven papers focused on adoption and monitoring. There is inadequate research focusing on investigating activity and diet tracking concerning diabetes management using IoT as only one paper mentioned it. This is because little is known about the potential of using applications to change health behaviors for disease prevention [20]. Eight of the research articles focused on the opportunities and challenges of IoT in health care (4C). Five of the articles in (4A) focused on adoption in conjunction with opportunities and challenges.

4.5 Healthcare Facility (HCF)

Four studies were conducted in a hospital facility, while three studies were conducted at home. Only one article focused on rehabilitation centers/old people's homes. More healthcare facility focus studies are required as twelve studies did not mention where the research occurred (5D). Investigating HCF enables one to have a clear understanding of the concept of IoT and to address the issues of adoption as a whole successfully.

4.6 Framework

One study investigated its study through the lens of the DoI theory as their research framework (7C), but it was used in combination with another theory. Three studies used a combination of models (7D), while two studies utilized frameworks not specified in our classification framework (7F). The existing literature shows that while some studies use a research framework to identify the factors influencing the adoption of IoT, many (ten) did not utilize theoretical frameworks. There is a need to investigate why some studies are not utilizing theoretical frameworks and why certain frameworks are preferred over other frameworks.

5 Discussions

This section discusses the research questions posed in this systematic literature review. ***RQ1: What are the opportunities, key challenges, and research gaps in IoT Diabetes monitoring?***

5.1 Opportunities

Twelve papers identified and discussed opportunities and challenges as part of their research. The use of IoT in diabetes monitoring reduces travel costs [21]. Continuous monitoring reduces morbidity and premature mortality caused by diabetes as it is automated and able to diagnose treatment outcomes [22]. The absence of human intervention in the adoption of IoT reduces the incidence of medical errors since data is collected automatically [23]. There is also patient satisfaction since the patient is actively involved in the treatment process and is assured that their medical data is being sent to the doctor automatically for analysis [22]. IoT helps patients in the exact usage of drugs as well as pharmacies and healthcare centers to prevent drug waste [22]. This presents a linked network between practitioner, pharmacy, and patient in real time. Furthermore, IoT can be used to assess the risk of new drugs like allergic reactions and undesirable drugs [22]. The implementation of IoT in health care has enabled more integrated and interoperable healthcare services [24]. Patients and medical staff have easy access to medical records and related information, thus, improving the quality and effectiveness of service [25].

5.2 Key Challenges

MHIoT can consist of many costly devices that must comply with regulatory and legal issues and may be out of reach to many consumers and health facilities especially in developing countries such as Malaysia [11]. Another challenge is security where confidential patient information can be hacked and used against the doctor and misdiagnose patients [25]. The devices can also run out of power, and this results in a denial of service (DoS) in healthcare data leading to inconsistency problems [26]. Healthcare systems also have to deal with both device interoperability and data heterogeneity in the IoT ecosystem [23]. Heterogeneity and interoperability are key limitation for IoT success due to the unavailability of universal standards leading to confidentiality, transparency, and reliability issues. There is also a lack of adequate training concerned with the configuration and usage of IoT devices, thus giving false or incorrect results [23]**.** Technology and algorithmic bias are also high as there is a perception that technology works on a certain kind of people.

To answer the second research question framed, ***RQ2: What are the theoretical frameworks that have been adopted in IoT Diabetes monitoring?***

Technology Acceptance Model [27]. In some studies, TAM was combined with other theories because its constructs and variables alone may not be enough. Therefore, there is a need to integrate it with other models which include social change processes like DOI. **Diffusion of Innovations Theory**: The DOI model was used to explain the success or failure of innovation in one of the research papers [28]. It can be noted that most of the theories applied in IoT are all concerned about the acceptance of IoT in the medical domain. The model is also criticized to be incomplete just like TAM [29]. **Unified Theory of Technology Acceptance and Use of Technology**: The UTAUT model can predict ICT usage within a consumer context; thus, it was preferred by some studies [30]. **Value-Based Adoption Model (VAM)**: One study applied the VAM to examine the influences of benefits and sacrifices on the user's perceived value of and intention to use IoT services in Taiwan [31]. Furthermore, in the VAM, other values such as performance value, emotional value, value-for-money, and social value should be explored to perceive their effect on adoption [32]. **Combination of Models**: The adoption of IoT from a multiple theory perspective is still lagging [33]. TAM and UTAUT were used in combination in one of the research studies [34]. Other studies combined DOI and TAM and revealed that respondents are ready to adopt IoT-enabled healthcare application, but the lack of IoT-enabled healthcare applications becomes a barrier for them to adopt it [11].

6 Conclusions, Research Gaps, and Future Work

This paper contributed to the research community by highlighting the challenges, opportunities, and theoretical frameworks that have been adopted in the monitoring of diabetes using IoT guided by two research questions. The findings reveal that remote monitoring of diabetes using IoT is limited in developing nations and dominated by work done in Europe and Asia only. An opportunity for future studies exists to study resource-constrained contexts especially in the African origin because it has been noted that it will be one of the leading continents with a high diabetic population and its resources are inadequate to cater for such a disease [17]. Secondly, there is a phenomenological difference between developed and developing countries; therefore, geographical contexts should be considered when carrying out this research, e.g., in Saudi Arabia, females are restricted by culture to communicate in any form with a man they are unrelated to [35]. Therefore, research needs to be conducted in other settings with different cultures and socioeconomic backgrounds. A cross-cultural investigation of IoT adoption may reveal other relevant factors as studies in this domain have not considered consumers in diverse geographical contexts [36]. Khumalo [37] is in accord with these studies as he notes that IoT must address very specific and evidence-based health "needs" of each context; the shortage of health experts; and the required skills to produce healthcare experts in developing nations. Furthermore, it is imperative to consider the perceptions of non-technical health workers as studies in this review did not consider them. More research on privacy and security regulations on IoT use in health care is required. Such research may also include cybersecurity protection tools, cloud vulnerabilities, and over-the-air (OTA) vulnerabilities. Also, research can be done on cost analysis to investigate if high-cost technologies can be substituted with low-end devices like cloud storage and data analytics technologies. Future research can also be done to come up with more robust frameworks to cater to future investigations in the domain. Preliminary findings indicate that there are limited frameworks for IoT adoption in diabetes [8, 11]. Frameworks that exist have been for Indian hospitals and hospitals in developed nations from an organizational and healthcare perspective without the diabetes context [38]. More frameworks are required as new technologies are emerging where features and utility of the technology, the context of usage, and the user technology need to be considered. A review of existing literature shows that a combination of theories can deliver more and offer in-depth solutions [32]. Research gaps concerning understanding the impact of awareness, privacy, and security concerns need to be addressed to be able to assess the readiness and adoption of IoT by resource-constrained contexts. Furthermore, policymakers should make sure that there is data-free access to diabetes Internet-based applications for more awareness [39]. Lastly, there is a need to understand the effects of relative advantage and awareness to assess the readiness of adopting IoT in resource-constrained contexts as the majority of the research studies discussed the opportunities and challenges of IoT from a general perspective and not specific to contextual needs. People still lean on the traditional ways of treating chronic diseases. More research output should be done for resource-constrained communities in Africa. The systematic review is limited in that its emphasis is on resource-constrained contexts. Further research is needed to analyze other contexts.

References

1. Tripathi S (2019) System dynamics perspective for adoption of Internet of Things: a conceptual framework. In: 2019 10th international conference on computing, communication and networking technologies. ICCCNT 2019, pp 1–10. https://doi.org/10.1109/ICCCNT45670.2019.8944664
2. Wei S, Zhao X, Miao C (2018) A comprehensive exploration to the machine learning techniques for diabetes identification. In: Proceedings of IEEE World Forum Internet Things, WF-IoT 2018, vol 2018, pp 291–295. https://doi.org/10.1109/WF-IoT.2018.8355130
3. Agyemang C et al (2016) Obesity and type 2 diabetes in sub-Saharan Africans—is the burden in today's Africa similar to African migrants in Europe? The RODAM study. BMC Med 14(1):166
4. Martínez-caro E, Cegarra-Navarro JG, García-pérez A, Fait M (2018) Healthcare service evolution towards the Internet of Things: an end-user perspective. Technol Forecast Soc Change 136(2018):268–276. https://doi.org/10.1016/j.techfore.2018.03.025
5. Sharma R, Kshetri N (2020) Digital healthcare: historical development, applications, and future research directions. Int J Inf Manage 53:102105. https://doi.org/10.1016/j.ijinfomgt.2020.102105
6. Mapa-Tassou C, Katte J-C, Mba Maadjhou C, Mbanya JC (2019) Economic impact of diabetes in Africa. Curr Diab Rep. 19(2):5. https://doi.org/10.1007/s11892-019-1124-7
7. Kelly JT, Campbell KL, Gong E, Scuffham P (2020) The Internet of Things: impact and implications for health care delivery. J Med Internet Res 22(11). https://doi.org/10.2196/20135
8. Kim SS, Kim SS (2018) User preference for an IoT healthcare application for lifestyle disease management. Telecomm Policy 42(4):304–314. https://doi.org/10.1016/j.telpol.2017.03.006
9. Zahedul M, Hoque R, Hu W, Barua Z (2020) Factors influencing the adoption of mHealth services in a developing country: a patient-centric study. Int J Inf Manag 50:128–143. https://doi.org/10.1016/j.ijinfomgt.2019.04.016
10. Costea-Marcu I-C, Militaru G (2019) Patients' attitudes toward the use of IoT medical devices: empirical evidence from Romania. In: Proceedings of the international conference on business excellence, vol 13, issue no 1, pp 567–577. https://doi.org/10.2478/picbe-2019-0050
11. Yuan YS, Cheah TC (2020) A study of internet of things enabled healthcare acceptance in Malaysia. J Crit Rev 7(3):25–32. https://doi.org/10.31838/jcr.07.03.04
12. Tripathi S, Pandit L (2019) analysis of factors influencing adoption of Internet of Things: a system dynamics approach. Theor Econ Lett 9(7):2606–2625. https://doi.org/10.4236/tel.2019.97164
13. Brous P, Janssen M, Herder P (2020, September) The dual effects of the Internet of Things (IoT): a systematic review of the benefits and risks of IoT adoption by organizations. Int J Inf Manage 51:101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008
14. Roy A, Zalzala AMSS, Kumar A (2016) Disruption of things: a model to facilitate adoption of IoT-based innovations by the urban poor. Procedia Eng 159:199–209. https://doi.org/10.1016/j.proeng.2016.08.159
15. Denyer D, Tranfield D (2009) Producing a systematic review. The SAGE handbook of organizational research methods, pp 671–689. https://doi.org/10.1080/03634528709378635
16. Amui LBL, Jabbour CJC, de Sousa Jabbour ABL, Kannan D (2017) Sustainability as a dynamic organizational capability: a systematic review and a future agenda toward a sustainable transition. J Clean Prod 142:308–322. https://doi.org/10.1016/j.jclepro.2016.07.103
17. Federation I (2019) IDF diabetes Atlas. Belgium, Brussels. [Online]. Available https://www.diabetesatlas.org
18. Thales Data Report, 2017. [Online]. Available http://enterprise-encryption.vormetric.com/rs/480-LWA-970/images/Thales_2017_Data_Threat_Report-Global_Edition.pdf
19. Venkatesh V, Morris M, Davis G, Davis F (2003) User acceptance of information technology: toward a unified. MIS Q 27(3):425–478
20. Schoeppe S et al (2016) Efficacy of interventions that use apps to improve diet, physical activity and sedentary behaviour: a systematic review. Int J Behav. Nutr Phys Act 13(1). https://doi.org/10.1186/s12966-016-0454-y

21. Rodbard D (2016) Continuous glucose monitoring: a review of successes, challenges, and opportunities. Diabetes Technol Ther 18(S2):S23–S213. https://doi.org/10.1089/dia.2015.0417
22. Alansari Z, Anuar NB, Kamsin A, Soomro S, Belgaum MR (2018) The Internet of Things adoption in healthcare applications. In: 2017 IEEE 3rd international conference on engineering technologies and social sciences (ICETSS) 2017, vol 2018, pp 1–5. https://doi.org/10.1109/ICETSS.2017.8324138
23. Selvaraj S, Sundaravaradhan S (2020) Challenges and opportunities in IoT healthcare systems: a systematic review. SN Appl Sci 2(1):1–8. https://doi.org/10.1007/s42452-019-1925-y
24. Longva AM, Haddara M (2019) How can IoT improve the life-quality of diabetes patients? MATEC web conference, vol 292, p 03016. https://doi.org/10.1051/matecconf/201929203016
25. Ndubuaku M, Okereafor D (2015, November) Internet of things for Africa: challenges and opportunities. In: 2015 international conference on cyberspace governance—CYBER-ABUJA2015, vol 9, pp 23–31. https://doi.org/10.13140/RG.2.1.2532.6162
26. Tuwanut P, Kraijak S (2016) A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. pp. 1–6. https://doi.org/10.1049/cp.2015.0714
27. Davis FD (1986) A technology acceptance model for empirically testing new end-user information systems: Theory and results. Sloan School of Management, Massachusetts Institute of Technology
28. Mishra V, Naik MKP (2017) Uses of wireless devices and IoT in management of diabetes. In Proceedings of national conference on emerging trends in science, technology & management (pp. 14–21)
29. Rogers EM (2010) Diffusion of innovations. 4th Edition, Simon and Schuster, New York
30. Venkatesh V, Thong JY, Xu X (2016) Unified theory of acceptance and use of technology: A synthesis and the road ahead. J Assoc Inf Syst, 17(1)
31. Hsu C, Lin JC (2018) Exploring factors affecting the adoption of Internet of Things services. J Comput Inf Syst 58(1):49–57. https://doi.org/10.1080/08874417.2016.1186524
32. Canhoto AI, Arp S (2017) Exploring the factors that support adoption and sustained use of health and fitness wearables. J Mark Manag 33(1–2):32–60. https://doi.org/10.1080/0267257X.2016.1234505
33. Mital M, Chang V, Choudhary P, Papa A, Pani AK (2018) Adoption of Internet of Things in India: a test of competing models using a structured equation modeling approach. Technol Forecast Soc Change 136:339–346. https://doi.org/10.1016/j.techfore.2017.03.001
34. Kao YS, Nawata K, Huang CY (2019) An exploration and confirmation of the factors influencing adoption of IoT-basedwearable fitness trackers. Int J Environ Res Public Health 16(18). https://doi.org/10.3390/ijerph16183227
35. Alkhudairi B (2016) Technology acceptance issues for a mobile application to support diabetes patients in Saudi Arabia. [Online]. Available http://search.ebscohost.com/login.aspx?direct=true&db=ddu&AN=0344E52E73DAC8E7&site=ehost-live&authtype=ip,uid
36. Nord JH, Koohang A, Paliszkiewicz J (2019) The Internet of Things: review and theoretical framework. Expert Syst Appl 133:97–108. https://doi.org/10.1016/j.eswa.2019.05.014
37. Khumalo NB (2017) The need for the establishment of E-records and eHealth legislation and policy framework in the health sector in Zimbabwe. Libr Philos Pract 1662:1–19
38. Dash SP (2020) The impact of IoT in healthcare: global technological change & the roadmap to a networked architecture in India. J Indian Inst Sci 100(4):773–785. https://doi.org/10.1007/s41745-020-00208-y
39. Gupta PK, Maharaj BT, Malekian R (2016) A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres. Multimed. Tools Appl 76(18):18489–18512

Application of Sound of Kobyz in Online Therapy and Health Improvement

Kumyszhan Mukasheva and Engelika Zhumataeva

Abstract Due to the tense modern rhythm of life, environmental, economic and social problems, there is an alarming trend toward an overall increase in mental illness and psychological disorders (Gusakova in Musical-therapeutic potential of elementary music-making and individual improvisation activity. I International Scientific and Practical Conference "Music and Health". Collection of reports and abstracts M.: National Association of Music Therapists, p. 31, 2009). Therefore, the search for new non-drug methods of psychological correction and health improvement of the population is the most urgent modern task. Recently, methods of music therapy have become more and more widespread. The author of the method has released a therapeutic disk "Gylkobyzdyn shipasy", which includes seven compositions reproduced by the author. The novelty of this research lies in the study of psychological, physiological and ethnocultural aspects of the use of the ancient Kazakh musical instrument Kobyz for health purposes. "Kobyztherapy" is a universal, progressive method of online recovery in areas such as psychology, sociology, health care and the social sphere, especially in the current COVID-19 pandemic.

Keywords Kobyztechnology · Kobyztherapy · Innovation · Music education · Music · Kobyz · Online consultation · Business consultation · Music therapy · Pedagogy and psychology · Universal application · Health improvement · Therapy

1 Introduction

For a century, infectious diseases have been the scourge of mankind; the epidemic of plague, smallpox and cholera devastated cities and villages. Situation changed in the 21st century, the so-called diseases of civilizations or diseases of adaptation came to the fore. "Diseases of the century" include diseases of blood vessels, bronchi,

K. Mukasheva (✉) · E. Zhumataeva
Toraigyrov University, Lomov str.64, 140007 Pavlodar, Kazakhstan
e-mail: kumiszhan.mukasheva@gmail.com

E. Zhumataeva
e-mail: kobyztherapy@list.ru

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_58

joints, stomach and intestines. These diseases are psychosomatic; social and psychological factors are actively involved in their development and course. In the current situation associated with mandatory quarantines, due to the declared pandemic, the load on the nervous system of the human psyche is increasing throughout the world. The information boom, the negative dynamics of interpersonal relations lead to the formation of emotional stress, which is one of the factors in the development of diseases. Life in conditions of indefinite quarantine has led to a radical change in the established stereotypes of behavior, which increases the level of anxiety, concerns for their future, for the future of their children and relatives.

By now, the material world we live in has reached significant development and is quite complex. This world brings more and more invasion and changes not only in

people's the way of life, but also in many mental and body processes. These are the consequences of such "restructuring":

- acceleration of the rhythm of life;
- a huge increase in the production and consumption of psychoactive drugs (sleeping pills, sedatives, tonic, stimulating, etc.);
- an increase in the production and consumption of psychoactive narcotic substances (alcohol, drugs, toxicants).

The acceleration of the pace of life led to a significant increase in stress load. The most sad consequences of this: a significant increase in mental disorders, suicides and psychogenic diseases. Therefore, the search for new non-medicinal methods of psychological correction and health improvement of the population is the most urgent modern task in recent years; methods of music therapy, introduced into the methodological foundations of music education of university students, are becoming more widespread.

What allows a person to find and maintain peace of mind, manage their passions or be inspired by future actions? It is the revival of Kobyztherapy—the cultural heritage of our people, accumulated over the centuries, which strengthens the psychological stability of the individual and spiritual development.

2 Kobyztherapy

2.1 Kobyz

The term kobyz (from the Turkic word "kobza") means an ancient, bowed instrument, the sound of which was used in the treatment of various diseases in the history of healing of the Kazakh people [1]. The term "therapy" (in Greek "therapeia") means care, treatment. Kobyztherapy is a trance method that expands access to unconscious information, which makes it possible to master new forms of its processing to activate a person's sanogenic resources. The author's technique "Kobyztherapy" has been practiced by the author for 19 years and gives positive results.

The emergence of the musical art of the Kazakh people, according to legend, is associated with the name of the legendary musician Korkyt. The people also call him the creator of one of the most ancient musical instruments of the East—kobyz.

Kyl-kobyz (from the Kazakh language—an instrument with hair strings) belongs to the common Turkic musical instruments, first mentioned in the well-known dictionary of M. Kashgari (11th century). According to legends, it was invented in the 7th-8th centuries.

Korkyt was the first “bucks” (meaning healer) who composed the first melody. Nar-kobyz is an indispensable attribute of the ritual and ceremonial practice of “bucks" and “zhyrau” (diviner). The kobyz instrument belongs to the bowed instrument family (1st millennium AD).

The “Kobyztherapy” method is used to treat and prevent a wide range of disorders, in particular: developmental deviations, emotional instability, behavioral disorders, spinal cord injury, psychosomatic diseases, internal diseases, mental deviations and autism.

2.2 Structural Features and Manufacturing Technique of Kobyz

Hollowed-out body is made in the form of a bowl; neck and resonator are one whole; neck is without frets; the top is made of camel or calfskin; the bow-shaped bow and strings are made of a horse tail (Fig. 1).

The hollowed-out body in the shape of a bowl is made of black pine, white young birch, maple, walnut, elm, saxaul, ebony, mahogany; the top deck is made of the skin of a camel or a goat.

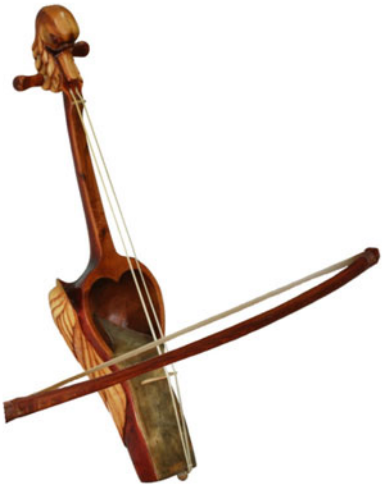


Fig. 1 Kobyz instrument

Tiek—the support for the strings—is made from the horn of a mountain goat, steppe roe deer and from cow or camel tibia bone; the strings and bow-shaped bow are made of a horse’s tail (five-year-old stallion).

2.3 Kobyztherapy Methodology

The author’s methodology “Kobyztherapy” was developed and tested by Kumyszhan Kairgalievna Mukasheva—Master of Psychology, music therapist, clinical and practicing psychologist, Member of the Association of Music Therapists of Russia, Member of the European Association of Music Therapists, Member of the Association Music and Medicine of the USA, Member of the Imaton Psychological Club in St. Petersburg, licensed specialist in folk and alternative medicine, Ph.D. candidate in psychology studies.

The main goal of the author’s methodology “Kobyztherapy” is the national basis for the spiritual development of a person through kobyz music at an innovative level.

The author of the method has released a therapeutic disk “Gylkobyzdyn shipasy”, which includes seven compositions reproduced by the author.

1. “Baқsynyk oyyny”, “Dance of the Baқsa”.
2. “Tүner-tүneruden aғaru, rukhani zhanғyru”, “Eclipse—Enlightenment”.
3. “Ata mura-ata tek”, “Genetic code—Call of the ancestors.”
4. “Қorқytyң saryny”, “Saryn of Korkyt”.
5. “Ұshyқtau”. “Energetic, spiritual cleansing.”
6. “Tənirge tabynu”. “Worship” of the Forces of nature: “Fire”—“From”.
7. “Dala Kueni”, Forces of nature “Freedom of the steppe”.

During the recording of the album, all seven compositions were put on arrangement, accompanied by natural sounds, for example: the murmur of a stream, the sound of the waves of the sea, the sound of the wind, etc., which has a huge impact on the activity of the brain. The very sound of kobyz compositions, performed in the form of kuyis, saryns, zikirs, has long been referred to as trance therapy.

It is important to highlight the fact that kobyz therapy is ethnic music, as the most “ancient medicine” of the rest known in the world (e.g., the music of shamans, qigong, Tibetan bells, sounds made when breathing by a person, the sound of a pulse, etc.).

Listening to the entire album helps to harmonize the psyche, to activate the processes of self-regulation in the body. Listening to this music album sets in motion, removes numerous negative deposits in the human psyche and contributes to the solution of many problems at various conscious and unconscious levels.

The Kobyztherapy program uses the author’s therapeutic compositions. Conducting individual online consultations, group online webinars contribute to the integration of the individual, the development of creative abilities, the expansion of consciousness, the improvement of interaction with the outside world and complete recovery.

"Kobyztherapy" is planned to implement programs for digital psychological counseling, health improvement of the population in the context of "health protection", providing for individual and group online counseling.

3 Advantage of Kobyzotechnology Programs in Universal Application: Health Care

This technology uses unique know-how, embodied in special music therapy programs. These programs are controlled and broadcast through the acoustic system "Kobyztherapy" to the hearing organs and at the same time to problem areas of the skin, which are covered with special membranes.

In membranes, which can be impregnated with cosmetic products to enhance the effect, acoustic and secondary electromagnetic fields are spread over the entire surface. They themselves penetrate the skin, enhance the depth of penetration into the skin of cosmetic products and stimulate the regeneration processes.

Kobyztherapy is an innovative technology for healing and rejuvenating the skin related to music therapy (MT)—a dynamically developing area of health care that uses more than 50 different musical and acoustic methods and approaches to correct mental and physical health, prevent diseases, social rehabilitation, creative and spiritual development of the individual.

In medicine, MT therapy technologies are used primarily for psychological and physiological correction, relieving pain syndromes, restoring reduced or lost functions, which has already found wide application in the clinic of internal diseases, in spa practice, in surgery and medical rehabilitation.

The use of integrative approaches and non-standard technical solutions in Kobyztherapy made it possible to achieve complex results of healing against the background of psychoemotional correction. The developed "software and hardware complex" Kobyztechnology has become an accessible and convenient tool for the practical implementation of technology at the modern level. This gives every reason to consider Kobyztherapy promising for widespread use in the practice of medical institutions.

4 Infrasound in Kobyztherapy

4.1 Purpose of the Study

In this article, for a deep and comprehensive understanding of the mechanisms of the effect of music on the human body, it is necessary to actively use the knowledge accumulated by acoustics, the field of physics that studies the properties of sound, elastic vibrations and waves that arise and propagate in gases, liquids and solids, perceived human ear. The frequency limit of sound perception has been established—from 16 to 20,000 Hz.

Sound vibrations with a frequency of less than 16 Hz, which are not perceived by the hearing organ, are called infrasound. Infrasound has an adverse effect on the human body, causing headache, fatigue, fear and increased irritability.

It is believed that the negative impact of infrasound is of a resonant nature. It was found that the purity of natural oscillations of the human body in the supine position is 3–4 Hz, while standing—5–12 Hz, chest—5–8 Hz, abdominal cavity—3–4 Hz [1].

Thus, the frequency range of infrasound, which is a driving force in relation to the body, has values close to the frequency of natural oscillations of individual systems and the body as a whole 132. Oscillations and waves, the frequency of which exceeds 20,000 Hz, which are also not perceived by the human ear, are called ultrasounds.

The upper limit of ultrasonic frequencies can be conventionally considered 109–1010. The limit is determined by intermolecular distances and therefore depends on the state of aggregation of the substance in which the ultrasonic wave propagates. Ultrasound is widely used in medicine for diagnostic and therapeutic purposes. The frequency spectrum of sounds used in music and reproduced by an ancient musical instrument—kobyz—as the main instrument for influencing the body lies in the frequency range not perceived by the human ear and therefore is the subject of primary interest in this study.

Infrasound is a mechanical vibration in the frequency range below 20 Hz. A characteristic feature of infrasound, in contrast to other mechanical vibrations, is a long wavelength and low vibration frequency. Due to the low absorption of energy, infrasound propagates over long distances from the source [2].

Of the many spectra of industrial and transport noises containing infrasonic components, three main types can be distinguished:

- Infrasonic—the highest sound pressure levels (SPL) are in the octave bands of geometric mean frequencies—2–26 Hz;
- Infra-low frequency—the highest SPL falls on the bands of average geometric frequencies—2–125 Hz;
- Low frequency—the maximum SPL is in the octave bands of 31.5–125 Hz. In a manufacturing environment, infrasound tends to combine with low-frequency noise and sometimes low-frequency vibration.

By the nature of the infrasound spectrum, broadband infrasound is distinguished, with a continuous spectrum more than an octave wide; harmonic, in the spectrum of which there are pronounced discrete components. The harmonious nature of infrasound is established in octave frequency bands by exceeding the level in one band, in comparison with neighboring ones, by at least 10 dB.

According to the temporal characteristics, a constant infrasound is distinguished, the sound pressure level of which on the “linear” scale on the “slowly” characteristic changes by no more than 10 dB during the observation time of 1 min; unstable, the sound pressure level of which on the “linear” scale on the “slow” characteristic changes by at least 10 dB during the observation time of at least 1 minute:

- for the characteristics of infrasound—octave sound pressure levels;
- for non-constant infrasound—the general sound pressure level on the "linear" scale of the sound level meter [3].

The bioresonance effect of musical influence on the human body is due to the phenomenon of resonance, as a general physical law of nature, according to which an external force, changing according to a periodic law and leading to the occurrence of forced vibrations of the body, and the amplitude of forced vibrations is directly proportional to the amplitude of the driving force.

At a certain frequency of the driving force, called resonance, the amplitude of the forced oscillations acquires a maximum value, which is why is it called resonance.

4.2 Materials and Method

The measurement of infrasound was carried out with a noise meter—"Noise meter integrating Ekofizika No. 100226", which passed certification No. BA 12-05-3280 dated June 21, 2012. The study was carried out by P. F. Kuznetsov, a laboratory assistant at the Department of EMF and other physical factors.

Infrasound measurements were carried out at the workplace of a music therapist. The measurement points were selected no more than 1 meter apart between the music therapist performing the musical compositions and the microphone. The microphone was positioned at a height of 1 meter from the floor and at a distance of at least 0.5 m from the laboratory doctor making the measurement.

Musical compositions were performed by a music therapist on four types of kobyz.

These are "small kobyz", "nar-kobyz", "kyl-kobyz" and "prima kobyz".

Further, the infrasound from the acoustic system (computer speakers) was measured; in this case, the author's composition of the kobyz therapy method was used: Forces of nature "Freedom of the Steppe", the conditions for measuring the acoustic system are similar to measuring musical instruments.

4.3 Discussion

By the nature of the infrasound spectrum, in this case, it is broadband infrasound with a continuous spectrum, 1/3 octave wide; harmonic. The harmonic nature of infrasound is established in octave frequency bands by exceeding the level in one band, in comparison with the neighboring ones, by at least 10 dB.

Sound pressure levels in dB 1/3 octave bands are the following in Hz:

"Small Kobyz"—67 Hz at a sound pressure level of 1.6 dB. "Nar-kobyz"—84, "kyl-kobyz"—66, "prima kobyz"—87, measurements of the acoustic system in the composition of the Force of Nature "Freedom of the Steppe"—62.

5 Conclusion

In connection with the tense modern rhythm of life, environmental, economic and social problems, there is an alarming trend toward a general increase in mental illness and psychological disorders [4]. Therefore, the search for new non-drug methods of psychological correction and health improvement of the population is the most urgent modern task. Recently, methods of music therapy have become more and more widespread.

The novelty of this research lies in the study of psychological, physiological and ethnocultural aspects of the use of the ancient Kazakh musical instrument kobyz for health purposes.

The results of measuring the infrasound of kobyz, as well as the acoustic system in the author's composition of the Forces of Nature "Freedom of the Steppe", showed the complete absence of discrete components. Harmonic vibrations and a low level of intensity have a beneficial effect on the human body as a whole.

Sound-reproducing devices, in this case the acoustic system in the author's composition Forces of Nature "Freedom of the Steppe", directly affect the skin and in the projection of vital organs. Sound signals, in full accordance with physical laws, falling into resonant frequencies, cause maximum vibration, exerting a direct kobyzotherapeutic effect on the organs.

Thus, the results of the study confirm that the author's method of Kobyztherapy meets the hygienic standards for the level of noise and infrasound, approved by the order of the Minister of Health of the Republic of Kazakhstan [5].

This study has shown that the method of Kobyztherapy can be successfully applied in preventive, experimental and clinical medicine as a new method of corrective targeted action on the functional activity of vital organs and a therapeutic effect on pathologically altered organs and tissues.

Therefore, the author's method of Kobyztherapy is proposed for introduction into the widespread practice of medical institutions, as one of the effective methods for mobilizing natural resources and adaptive capabilities of the human body.

"Kobyzotherapy" is a universal, progressive method of online recovery in areas such as psychology, sociology, health care and the social sphere, especially in the current COVID-19 pandemic.

References

1. Shusharjan SV (1998) Musical therapy and the reserves of the human body. Publishing house "Antidor", p 74
2. Sraubaev EN, Belonog AA (2008) Guidelines for sanitary examination in the field of occupational hygiene: teaching aid. SANAT-Polygraphy, Karaganda, p 178
3. Mukasheva KK (2011) Author's method "Kobyzotherapy". Certificate of State. registration No. 469 IS 0006581 issued by the Ministry of Justice of the Republic of Kazakhstan, the Committee on Intellectual Property Rights. Astana

4. Gusakova SV (2009) Musical-therapeutic potential of elementary music-making and individual improvisation activity. I International Scientific and Practical Conference “Music and Health”. Collection of reports and abstracts M.: National Association of Music Therapists, p 31
5. Hygienic standards. Approved by the order of the Minister of Health of the Republic of Kazakhstan dated 03.12.2004 No. 841 “On the approval of hygienic standards.”

Building a NoSQL ERP

Ela Pustulka, Stefan von Arx, and Lucia de Espona

Abstract Enterprise resource planning (ERP) systems are needed in many business activities. Small and medium enterprises (SMEs) are not well-served by current ERPs, as such systems are hard to tailor. This prompts us to experiment with building an ERP on top of a NoSQL database, which intends to be more flexible, as it is based on JSON and not on a relational data model. We present a novel ERP solution specifically designed to grow and evolve as the world changes. The ERP is for a service company which bills for time spent on customer projects. The work involves various challenges: data modelling, query specification, write and read performance analysis, versioning, user interface generation and query optimisation. Here, we report on the performance of a NoSQL ERP using MongoDB and show that writes are fast and queries and reports are fast enough.

Keywords ERP · Enterprise system · SME · NoSQL · MongoDB

1 Introduction

Enterprise resource planning systems (ERPs) have been an integral part of business organisations for decades [8, 10]. The global ERP market is around USD 38 billion [9], and small and medium enterprises (SMEs) are increasingly getting interested in acquiring an ERP system. The majority of such systems are based on relational database technologies. The advantages are clear: performance, data integrity and

E. Pustulka (✉) · S. von Arx · L. de Espona
FHNW University of Applied Arts and Sciences Northwestern Switzerland,School of Business, Institute for Information Systems, Olten, Switzerland
e-mail: elzbieta.pustulka@fhnw.ch

S. von Arx
e-mail: stefan_vonarx@hotmail.com

L. de Espona
e-mail: lucia.espona@fhnw.ch
URL: https://www.fhnw.ch

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_59

quality, security, advanced add on analysis tools and many others. However, ERPs are not flexible [8] and are expensive to buy and commission. Users need to be trained, and business processes often have to be modified to suit the system, or a system needs to be tailored to the business need [3, 31]. Current enterprise systems do not evolve easily and lag behind the business needs, as seen during the COVID epidemic which moved many businesses online [17].

NoSQL systems [23] are potentially flexible as they ingest data in JSON which can be easily extended with new data items, allowing us to evolve the data model. They are predominantly found in Big Data applications. Many open research questions arise with regard to NoSQL [7]. In terms of applications, there is no research on NoSQL ERPs. Existing NoSQL benchmarks include a MongoDB TCP-C [16] and TCP-H [19]. Further work compares the performance of NoSQL and a relational database for a small ERP [1, 27], geographic information [21] and statistical RDF [28]. Another MongoDB performance evaluation [30] explores document inlining. There is a growing interest in JSON storage in relational databases, including Oracle [18] or SAP HANA [11]. However, relational stores and ERP systems have not been designed primarily for SMEs but for large organisations. ERP adoption or upgrade [3] needs strategic thinking and preparation and is out of reach for an SME. Our business partner noticed a new opportunity and proposed to create am ERP for SMEs, based on JSON. As this is novel, we are exploring the use of currently the most popular NoSQL store, MongoDB, to offer flexibility, compliance, data governance, integrity, performance and other features needed in an ERP. We target SMEs which are poorly served by existing solutions. We present a billing scenario. A service company bills customers for work done on customer projects. We measure insert and query performance on 1 million time sheet entries on a local MongoDB running on a PC. Such a scenario is relevant, particularly in Switzerland, as financial details are too precious to be placed in the cloud. Our contributions are as follows. We show that writes are fast and queries often perform in under 100 ms, which feels instant to the user. MongoDB offers good support for query writing and optimisation. We confirm that our ERP delivers performance required in a simple SME scenario. Our measurement is a partial proof of the feasibility of using a NoSQL database as an ERP platform in this context.

The rest of the paper has the following structure. Sect. 2 reviews related work, and Sect. 3 presents the methods. Section 4 details the measurement, and Sect. 5 discusses and concludes.

2 Related Work

Recent ERP surveys look at critical success factors (CSFs) related to system characteristics, its acquisition and use. [13] found out that security, project management, communication, compliance, network speed and organisational resistance to change are most relevant. [22] concluded that increasingly non-technical factors such as people, skills, communication and governance are in focus, and not the frameworks, methodologies or models. [29] looked at evaluation frameworks and stated that user training, ERP integration and enhanced traceability are top priorities. The overall focus is on quality (security, business fit, performance and usability). We found no literature describing NoSQL ERPs.

NoSQL systems [23] are classified into key-value, document, graph and wide column stores. MongoDB is a document database [24]. Key-value storage performance is analysed in [14]. MongoDB's papers include [5, 6, 15, 16], with advice that schema normalisation does not lead to good performance.

Recent work investigates MongoDB performance improvements. [20] use remote direct memory access (RDMA). [2] study performance in a real-time cloud, as needed for online streaming and gaming. [12] consider the database as a service (DBaaS) scenario read optimisation. [4] study the performance of MongoDB drivers. [21] compare the performance of PostgreSQL to MongoDB on spatio-temporal data. PostgreSQL with PostGIS outperforms MongoDB but MongoDB indexing benefits performance more than in PostgreSQL. [30] focus on business intelligence (BI) and develop a heuristic which can help modellers to decide which data layout to use.

3 Methods

3.1 ERP System Architecture, Scenario and Data Model

Our system architecture consists of a database layer which includes versioning, AI-based query optimisation and tuning, middleware responsible for the business logic, and a user interface layer which generates a GUI. The database layer includes a write and query module we present here, a versioning package, a database optimisation agent based on [32], and a data quality (DQ) package.

We support the following scenario. 1. Employee inputs time sheet entry; 2. Employee reviews time sheets; 3. Manager reviews finance; 4. System reads time sheets to calculate the invoices and updates time sheets with status *billed*.

Figure 1 shows an ER model based on the JSON we received from business. The model imposes a data load order: customer, employee, project and service, followed by a time sheet, and invoice creation. Each invoice contains an embedded array of items derived from the time sheets, which is typical in NoSQL and serves to optimise performance by storing all the related data together; see [30].

3.2 Data, Measurement and Workload

JSON was generated using Faker [26]. We timed data load for customers, employees, projects and services. Then we looked up the IDs generated by MongoDB and created the time sheets which refer to the existing collections. Inserts used *insertMany()* and

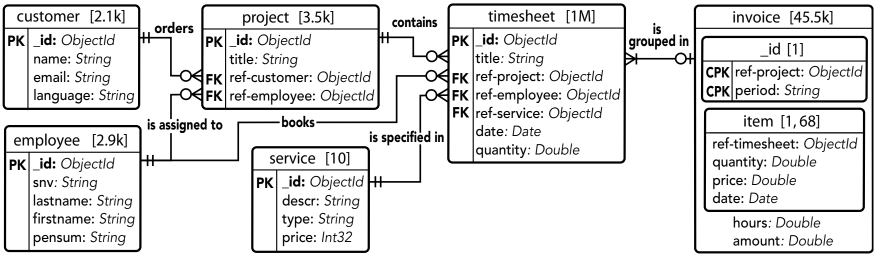


Fig. 1 Billing data include the customer, employee, project, service, time sheet and a derived relation invoice. An invoice holds items extracted from the time sheets embedded as an array. Relation headers show cardinalities

Table 1 Collection write performance (ms), average of 10 runs

	Service	Customer	Employee	Project	Time entry
Items	10	2100	2900	3500	1′000′000
Collection size KB	1	69	151	109	123′600
Index size KB	20	32	52	60	9400
Run 1 (cold) ms	28	108	113	109	10′442
Avg. for runs 2–9	11	83	97	96	10′470
Overhead % run 1	148	29	16	14	0

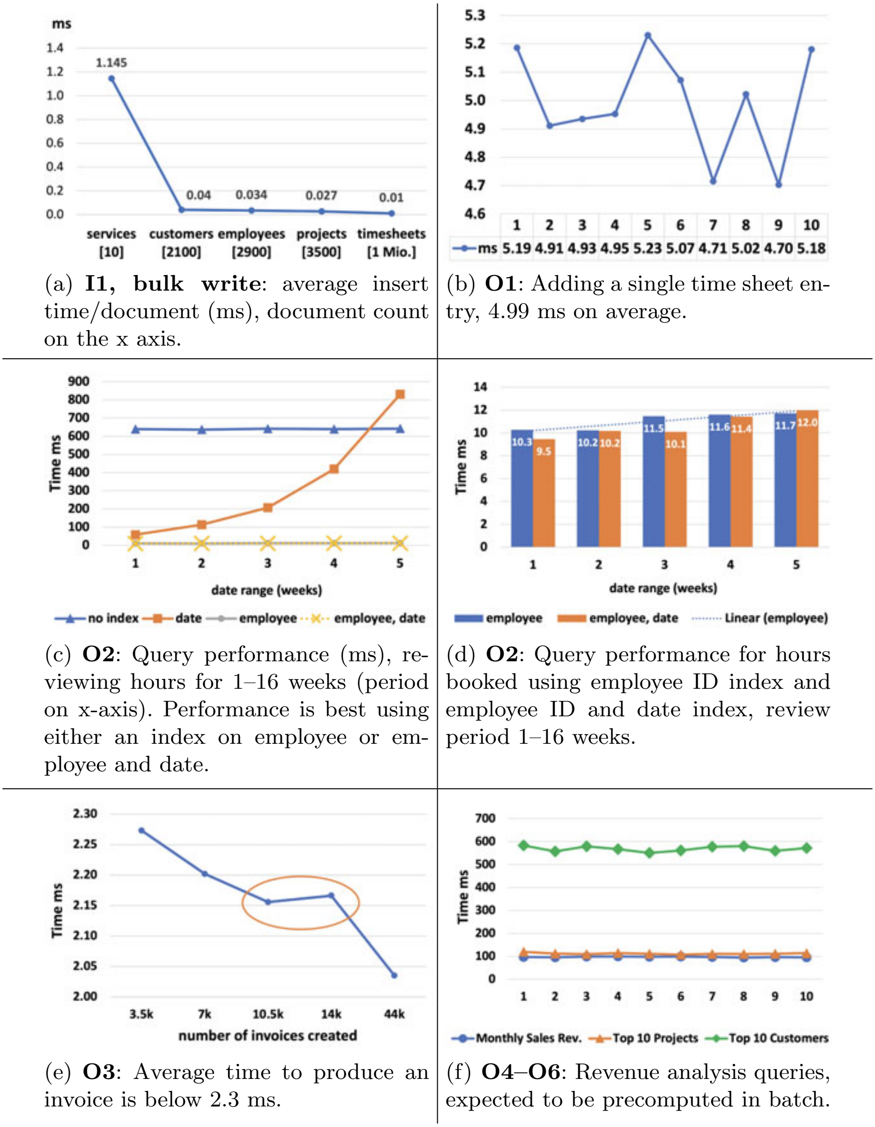
were timed by *process.hrtime()* directly and output to the console. We ran each test 10 times on a PC with AMD Ryzen 5 2600 6-core 3.4 GHz, 16 GB RAM, Samsung 860 Evo SSD, under Windows 10 Pro, MongoDB 4.4.0, with a stand-alone DB without a replica set.

We test the ERP with one year of business, 2900 employees and 35 managers. We start with a bulk insert **I1**, and see how long a migration or a data workhouse load takes. Further operations are numbered **O1** to **O6**. Time critical operations are in bold. The pipelines are shown in Table 2.

- **I1**: bulk write: customer, employee, service, project, 1 mln time sheet entries
- **O1: employees book** time sheet entries
- **O2: employees review** time sheet weekly
- **O3**: system generates invoices monthly, on average 83K time sheet entries per month, calculate totals and UPDATE 83K time sheets with $billed = true$
- **O4**: Managers check the invoices monthly
- **O5: Managers review** top 10 projects weekly
- **O6: Managers review** sales per customer weekly

Table 2 Data pipelines

	Operation and operation steps	Operators	Collection
O2: reviewing hours booked			
1	Filter by parameters *employee* and *date range*	$match	Timesheets
2	Aggregate hours, items by project	$group	
3	Add project name	$lookup $addFields	Projects
4	Format output	$project	
5	Sort by project with the highest hours	$sort	
O3a: Invoice generation			
1	Filter by the input parameter *date range*	$match	Timesheets
2	Add service rate and multiply by hours	$lookup $addFields	Services
	Aggregate hours and amount by project and month. List corresponding timesheets as items	$group	
4	Create materialised view	$merge	
O3b: Updating the invoiced time sheets			
1	Retrieve timesheet IDs from invoices	$project	Invoices
2	Bring IDs into a usable format	$unwind $replaceRoot	
3	Update retrieved timesheets with billed: *true*	*updateMany*	Timesheets
O4: Monthly sales			
1	Aggregate hours and amount by month	$group	Invoices
2	Sort by year, month	$sort	
3	Format output	$project	
O5: Top 10 projects			
1	Aggregate hours and amount by project	$group	Invoices
2	Sort by highest amount, limit to top 10	$sort, $limit	
3	Add project and project manager name	$lookup $addFields	Projects, employees
4	Format output	$project	
O6: Top 10 customers			
1	Filter by the input parameters *month* and *year*	$match	Invoices
2	Add customer name	$lookup $addFields	Projects, customers
3	Aggregate hours and amount by customer	$group	
4	Sort by highest amount, limit to top 10	$sort, $limit	
5	Format output	$project	



(a) **I1, bulk write**: average insert time/document (ms), document count on the x axis.

(b) **O1**: Adding a single time sheet entry, 4.99 ms on average.

(c) **O2**: Query performance (ms), reviewing hours for 1–16 weeks (period on x-axis). Performance is best using either an index on employee or employee and date.

(d) **O2**: Query performance for hours booked using employee ID index and employee ID and date index, review period 1–16 weeks.

(e) **O3**: Average time to produce an invoice is below 2.3 ms.

(f) **O4–O6**: Revenue analysis queries, expected to be precomputed in batch.

Fig. 2 Performance. In **I1** the leftmost item (services) is the highest although the data volume is the smallest, as a new collection is created and the creation time is not amortised over the number of services. Another reason could be that it is a cold run. **O2**: EmployeeID index and employeeID and date index perform similarly. **O3**: Paging starts when more than 3 months' worth of invoices are to be created. The ellipse highlights the area where we allow paging. **O4–O6**: Two queries are fast enough (0.1 ms), and one is slower: candidate for batch

Table 3 **O3**: Average invoice creation times in s for periods from one month to a year

Months	Sheets	Invoices	Time s	Comment
1	83K	3.5K	7.96	
2	167K	7K	15.41	
3	250K	10.5K	22.63	
4	333K	14K	–	Out of memory
4	333K	14K	33.33	Paging allowed
12	1M	44K	89.47	Paging allowed

Typically, invoicing happens monthly

4 Results

I1, a bulk insert. In MongoDB, a collection is created when the first document is entered, so the first insert is slower than the following ones. Table 1 shows bulk write performance. A large time sheet collection has no overhead and a small one with 10 service items is slow. Overall write performance is satisfactory, as small collections are written within 0.1 s and the large collection needs 10.4 s; see Fig. 1. Insert times range from 1.145 ms per service to 0.01 ms for a time sheet entry.

O1 write a time sheet: Fig. 2 shows the performance of single time sheet writing which averages 4.99 ms (satisfactory).

O2: Reviewing Hours Booked An employee checks their time entries weekly, using pipeline **O2**; see Table 2. Without indexing, this is slow, averaging 640 ms. Figure 2 shows that adding an index on employee ID or a composite index on employee ID and date guarantee good performance. Comparison of those two indexing options is shown in Fig. 2. When using 1 mln time sheet entries, both options perform well, on average under 12 ms.

O3: Invoicing Invoicing is done in batches offline and consists of two pipelines, a query **O3a** and an update **O3b**; see Table 2. Normally, companies invoice weekly, fortnightly or monthly. Here, up to three months of invoicing is possible in memory. Upwards of three months, we allow paging, specifying *allowDiskUse: true*. Average creation time per invoice is below 2.3 ms; see Fig. 2. On average, an invoice sums up 83K time sheet entries per month, and the run needs 7.96 s, executing **O3a** and **O3b**, Table 2. Runs covering up to one year are shown in Table 3. This is satisfactory.

O4 to O6: Revenue Analysis.

O4, Sales revenue after invoicing, required monthly; see Table 2 .

O5, Top 10 projects, invoices aggregated by project; see Table 2.

O6, Top 10 customers; see Table 2
Figure 2 compares the performance of queries **O4** to **O6**. Monthly sales and top 10 projects perform well, around 100 ms. However, top 10 customers is slow, circa 600 ms, and the query should be precomputed as batch.

5 Discussion, Future Work and Conclusion

An ERP system for an SME has to perform well in three settings: manual data entry or update, interactive query and batch. [25] says the user will notice the system is slow when they wait longer than 100 ms, while in a batch scenario the speed is not so important. Our test includes writes and reads on a local PC where the performance satisfies the requirements. A system running locally might be preferable for some companies, to ensure that customer data remain on site, which is attractive to financial services.

We could optimise performance by using inlined collections. As the revenue analysis pipelines use no indexing yet, this will improve once an automated indexing algorithm we are working on is used. Other optimisation options involve using the cloud.

We have tested data models for human resources (HR) and other ERP areas. We are refining data versioning for compliance. Ongoing work is using machine learning to automate index selection, using [32]. We will automate data integrity and quality control. Our partners in the UX area are prototyping automated user interface generation.

We presented the first step on the road to create an ERP for an SME. We observe the ease of programming, good insert performance, acceptable query performance, and the need for further work in automated performance tuning and data quality. This encourages us to make further steps towards a flexible ERP system which can adapt as the company changes. *Experiment code is at* https://github.com/pier4all/data-generation. We acknowledge funding from the Innosuisse, grant 44824.1 IP-ICT.

References

1. Aboutorabi SH, Rezapour M, Moradi M, Ghadiri N (2015) Performance evaluation of SQL and MongoDB databases for big e-commerce data. In: 2015 international symposium on computer science and software engineering (CSSE), pp 1–7
2. Andreoli R, Cucinotta T, Pedreschi D (2021) RT-MongoDB: a NoSQL database with differentiated performance. In: Proceedings of 11th international conference on cloud computing and services science, CLOSER'21, SCITEPRESS, pp 77–86
3. Barth C, Koch S (2019) Critical success factors in ERP upgrade projects. Ind Manag Data Syst 119(3):656–675
4. Cayres LU, de Lima BS, Garcia RE, Correia RCM (2020) Analysis of Node.js application performance using MongoDB drivers. In: Information technology and systems: proceedings of ICITS, vol 1137 of advances in intelligent systems and computing. Springer, Berlin, pp 213–222
5. Daly D (2021) Creating a virtuous cycle in performance testing at MongoDB. In: ICPE'21: ACM/SPEC international conference on performance engineering (ICPE). ACM, pp 33–41
6. Daly D (2021) Performance engineering and database development at MongoDB. In: ICPE'21: ACM/SPEC international conference on performance engineering (ICPE). ACM, p 129
7. Davoudian A, Chen L, Liu M (2018) A survey on NoSQL stores. ACM Comput Surv 51:2 Apr
8. De Michelis G, Dubois E, Jarke M, Matthes F, Mylopoulos J, Schmidt JW, Woo C, Yu E (1998) A three-faceted view of information systems. Commun ACM 41(12):64–70 Dec

9. Faith T, Nguyen D, Torii D, Schenck P, Hestermann C (2020) Magic quadrant for cloud ERP for product-centric enterprises. https://www.gartner.com/doc/reprints?id=1-1ZB9RIQ1&ct=200624&st=sb
10. Gibson N, Holland CP, Light B (1999) Enterprise resource planning: a business approach to systems development. In: 32nd annual Hawaii international conference on system sciences HICSS-32. IEEE Computer Society
11. Guerrero S (2021) Consuming data in Fiori Applications. In: Custom Fiori Applications in SAP HANA. Springer, Berlin, pp 37–80
12. Huang C, Cahill MJ, Fekete AD, Röhm U (2020) Deciding when to trade data freshness for performance in MongoDB-as-a-service. In: 36th international conference on data engineering, ICDE'20. IEEE, pp 1934–1937
13. Huang Q, Rahim MM, Foster S, Anwar M (2021) Critical success factors affecting implementation of cloud ERP systems: a systematic literature review with future research possibilities. In: 54th Hawaii international conference on system sciences, HICSS 2021. ScholarSpace, pp 1–10
14. Idreos S, Callaghan M (2020) Key-value storage engines. In: Proceedings of 2020 ACM SIGMOD international conference on management of data, SIGMOD '20, ACM, pp 2667–2672
15. Ingo H, Daly D (2020) Automated system performance testing at MongoDB. In: Proceedings of 8th international workshop on testing database Systems, DBTest@SIGMOD 2020. ACM, pp 3:1–3:6
16. Kamsky A (2019) Adapting TPC-C benchmark to measure performance of multi-document transactions in MongoDB. Proc VLDB 12(12):2254–2262
17. Kim RY (2020) The impact of COVID-19 on consumers: Preparing for digital sales. IEEE Eng Manag Rev 48(3):212–218
18. Liu ZH, Hammerschmidt B, McMahon D, Chang H, Lu Y, Spiegel J, Sosa AC, Suresh S, Arora G, Arora V (2020) Native JSON datatype support: maturing SQL and NoSQL convergence in Oracle database. Proc VLDB 13(12):3059–3071
19. Llano-Ríos TF, Khalefa M, Badia A (2020) Experimental comparison of relational and NoSQL document systems: the case of decision support. In: Performance Evaluation and Benchmarking—12th TPC technology conference, TPCTC'20, vol 12752 of LNCS. Springer, Berlin, pp 58–74
20. Lu F, Fang T, Zhang Z, Li S, Chen J, An H, Han W (2019) Improving the performance of MongoDB with RDMA. In: 17th IEEE international conference on smart City; 5th IEEE international conference on data science and systems, HPCC/SmartCity/DSS19. IEEE, pp 1004–1010
21. Makris A, Tserpes K, Spiliopoulos G, Anagnostopoulos D (2019) Performance evaluation of MongoDB and PostgreSQL for spatio-temporal data. In: Proceedings of workshops of EDBT/ICDT'19, vol 322 of CEUR Workshop Proceeings
22. Marimuthu T, van der Merwe A, Gerber A (2021) Systematic literature review of essential enterprise architecture management dimensions. In Proceedings of 6th international congress on information and communication technology—ICICT'21, vol 1, vol 235 of LNCS. Springer, Berlin, pp 381–391
23. Meier A, Kaufmann M (2019) SQL and NoSQL databases. Springer, Berlin
24. MongoDB I (2021) MongoDB. https://www.mongodb.com
25. Nielsen J (1993) Usability engineering. Morgan Kaufmann, Amsterdam
26. NPMFaker (2021) Faker.js—generate massive amounts of fake data in the browser and node.js. https://www.npmjs.com/package/faker
27. Parker Z, Poe S, Vrbsky SV (2013) Comparing NoSQL MongoDB to an SQL DB. In: ACM Southeast regional conference 2013, SE'13. ACM, pp 5:1–5:6
28. Ravat, F, Song J, Teste O, Trojahn C (2020) Efficient querying of multidimensional RDF data with aggregates: comparing NoSQL, RDF and relational data stores. Int J Inf Manag 54:102089
29. Senaya SK, van der Poll JA, Schoeman M (2022) Towards a framework to address enterprise resource planning (ERP) challenges. In: Proceedings of 6th international congress on information and communication technology. Springer, Berlin, pp 57–71

30. Soransso RASN, Cavalcanti MC (2018) Data modeling for analytical queries on document-oriented DBMS. In: Proceedings of 33rd annual ACM symposium on applied Computing, SAC'18, pp 541–548
31. van Beijsterveld JA, Van Groenendaal WJ (2016) Solving misfits in ERP implementations by SMEs. Inf Syst J 26(4):369–393
32. Wang J, Trummer I, Basu D (2021) UDO: universal database optimization using reinforcement learning. Proc VLDB 14(13):3402–3414

Models for Estimation of Concrete Compressive Strength Based on Experimental Research with Destructive and Non-destructive Methods

Ivan Ivanchev

Abstract This article presents experimental studies for assessing the concrete compressive strength in existing reinforced concrete members with destructive and non-destructive methods. For the destructive tests, 12 cube test specimens and 12 reinforced concrete beams (from which, 11 cores were drilled) were prepared in one day with the same recipe composition of the concrete. For two years, the reinforced concrete members were indoors, and in the following years, they were left outdoors exposed to external atmospheric influences. The research is aimed at the combined use (SonReb method) of two non-destructive methods: the method of elastic rebound (Schmidt rebound hammer) and ultrasonic pulse velocity method (UPVM) in order to achieve greater accuracy in assessing the compressive strength of concrete. Models have been developed describing the correlation between the determined compressive strength in the destructive test of cubes and cores with the measured rebound number and ultrasonic pulse velocity for the age of the concrete 1126th and 1926th day. The analysis was performed in Microsoft Excel environment.

Keywords Concrete · Compressive strength · Destructive · Non-destructive testing · SonReb

1 Introduction

One of the most important mechanical properties, which is important in design of reinforced concrete members and when determining their bearing capacity is the compressive strength of concrete [1]. The compressive strength changes over time and this requires monitoring during service. Methods for assessing the concrete compressive strength are destructive and non-destructive. The most reliable are the destructive methods, in which standard test specimens [2], prepared during the construction of the reinforced concrete members, or cores drilled from the existing reinforced concrete structures that are in operation are tested. Other methods are non-destructive testing

I. Ivanchev (✉)
University of Architecture, Civil Engineering and Geodesy (UACEG), Sofia, Bulgaria
e-mail: ivanchev_fce@uacg.bg

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_60

(NDT) techniques and widely used in practice are the methods of elastic rebound, ultrasonic pulse velocity method (UPVM), ultrasonic pulse echo method, and others. Non-destructive tests are cheaper, less time-consuming, do not violate the integrity of the structure [3], but give an indirect assessment, which is why they are influenced by many factors, and their results can be unreliable. It is often appropriate to be used a combination of destructive methods with several NDT techniques. The theoretical principle of the combination of several NDT techniques is that sometimes the factors have the opposite effect on the measurement results of the different methods. Combining the ultrasonic method with the method of elastic rebound is the most popular combination and is known as SonReb [4, 5].

This paper examines the effectiveness of the combination of destructive and non-destructive techniques (rebound number determined with Schmidt hammer and ultrasonic velocity with UPVM).

2 Methods Used in Experimental Research

The following four methods were used in the experimental studies:

Method of elastic rebound (Schmidt Hammer) determines the surface hardness of concrete, and hence, the probabilistic compressive strength of concrete in new and existing reinforced concrete structures [2, 6–9]. The Schmidt hammer measures the magnitude of the elastic rebound of a spring-loaded steel body from a concrete surface. The measured rebound number is related to the surface toughness of the concrete. The test is sensitive and the results can be affected by the type of cement, the type of aggregate, curing and age of the concrete, surface condition, and moisture content of concrete surface, the carbonization of the concrete, and others.

Non-destructive ultrasonic pulse velocity method (UPVM) uses the propagation of ultrasonic waves introduced into concrete, where they propagate, dissipate, and are reflected from the boundary between two environments [8–12]. The measuring instruments consist of an ultrasonic oscillation generator, transmitter, receiver, amplifier, and reading device. The generator generates high-frequency signals with a frequency of 25–150 kHz. The transmitter is a piezoelectric crystal. The receiving piezoelectric transducer registers ultrasonic waves and converts them into electrical signals. From the ultrasonic signal velocity, probabilistic compressive strength can be determined.

SonReb Method makes it possible to apply the combination of the measurement re-sults with UPVM and the Method of elastic rebound [2, 13] with the obtained compres-sive strength in a destructive test of standard test specimens (prepared from the same concrete mix on the day of construction of the reinforced concrete members) or cores drilled from a reinforced concrete structure that is in operation. To assess the compressive strength, a correlation is sought between the independent variables (velocity of the ultrasonic signal and the magnitude of the rebound) and the dependent variable–compressive strength of the concrete [9, 14]. In the literature, many authors have reported empirical correlation formulas for relationship of concrete compressive strength f_c with non-destructive measurements of the rebound number and the ultrasonic velocity. The models obtained from them are linear, power, exponential, polynomial, or others. In cases where there is no data on the concrete used, an equation of the type is used [2, 3, 17]:

$$f_{c,\mathrm{SonReb}} = aR^b V^c, \tag{1}$$

where *a*, *b*, *c* are constants; *V*—ultrasonic pulse velocity; *R*—rebound number.

The coefficients *a*, *b*, and *c* in Eq. (1), and correlation curves between compressive strength and non-destructive test results can be obtained from the Excel regression analysis function [15]. The relationship between the compressive strength and NDT measurements is called "conversion model." The resulting iso-strength curves can give a correct prediction of the compressive strength of concrete and are adapted only to the specific case (specific reinforced concrete structure) for which they are derived [1].

Destructive methods are the most reliable way to assess the mechanical properties of concrete; although, they are significantly invasive [2]. They are applied on standard test specimens or on cores taken from reinforced concrete structures. The test specimens are tested for compression till failure on testing machines for materials. The load speed is constant. The load is applied to the test specimen without hit and increases evenly until failure; the force *F* is reported; the compressive strength f_c is calculated.

In this paper, the author aims to develop correlation equations and curves for determining the compressive strength of concrete in existing reinforced concrete beams, using destructive and non-destructive methods. Non-destructive and destructive testing are in accordance with European standards.

3 Experimental Setup

The specimens for determining the compressive strength of the concrete f_c on the 1126th and 1926th day of laying the concrete mix were prepared in one day of concrete with the same recipe composition (Fig. 1).

Part of the research was done on four series of reinforced concrete beams. The series differ in provided longitudinal reinforcement, concrete cover, and reinforcement ratio. Their structural parameters were selected so as to correspond to the characteristic parameters of the beams designed in practice in industrial and civil construction. They were prepared of concrete class C25/30, fine fraction of coarse aggregate ($d_{\max} = 12$ mm), and consistency S3. The reinforced concrete members were indoors for two years, and in the following years, they were left outdoors, exposed to external atmospheric influences.

For experimental study of the concrete strength, characteristics were prepared 12 cubes with dimensions 150/150/150 mm in the same day with the reinforced concrete beams. The cubes were tested at age 1126th day. They were made from the same

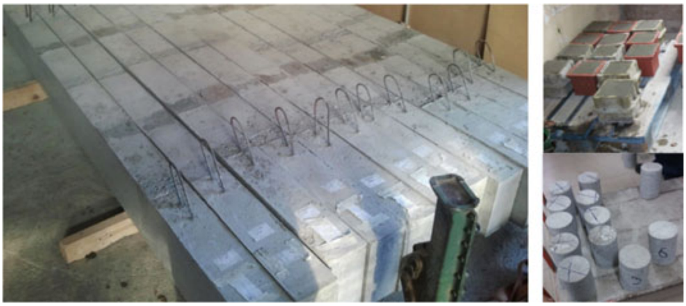


Fig. 1 Experimental specimens for non-destructive and destructive testing (personal archive)

recipe composition of concrete as for reinforced concrete beams. Their dimensions were chosen depending on the size of the coarse aggregate—EN 12390-1:2012. The specimens were prepared according to EN 12390-2:2009, and the sampling of the concrete mix was done according to EN 12350-1:2009.

To study the concrete compressive strength at age 1926th day, 11 cores with a diameter (D) Ø100 mm were taken from the beams at a depth ranging from 151 to 156 mm from places without visible cracks, pores, cavities, defects, and reinforcement on the surface of the beams [2, 16, 17]**.** The measurements were done with an accuracy of 1 mm. The choice of core diameter is regulated by the D/A ratio, where A is the maximum size of the coarse aggregate. According to EN 12504-1:2019, this ratio must be equal to or greater than 3, 0. The drilling of cores is in accordance with EN 12504-1:2019. In real conditions, the hole obtained when drilling the core is filled with concrete or other suitable fillers [1]. Before performing the tests, the selected 11 concrete test specimens (cores) were prepared by cutting off their ends on both sides, and they become cylinders with a depth of 100 mm and a diameter of 100 mm, i.e., the l/d ratio is equal to 1.

4 Tests and Results

For determining the compressive strength of concrete through its surface, hardness was determined the rebound number (Fig. 2a), according to EN 12504-2:2012 and a Digi Schmidt hammer was used. On the age of concrete 1126th day on each cube on two opposite sides, 10 hits were made. The distances between the centers of hits and from the edges of the cubes were not less than 30 mm. In each series of tests, the direction is horizontal. The rebound number varies in the range $R = 44$–49.5.

When testing the beams at age 1926th day on the two opposite sides in places where the cores will be drilled, 10 measurements were made by the method of elastic rebound. In each series of tests, the direction is vertical from top to bottom. Each mark on the surface was checked after the rebound, and if the hit had fallen on a surface pore, the result was not taken into account. The median value of the rebound

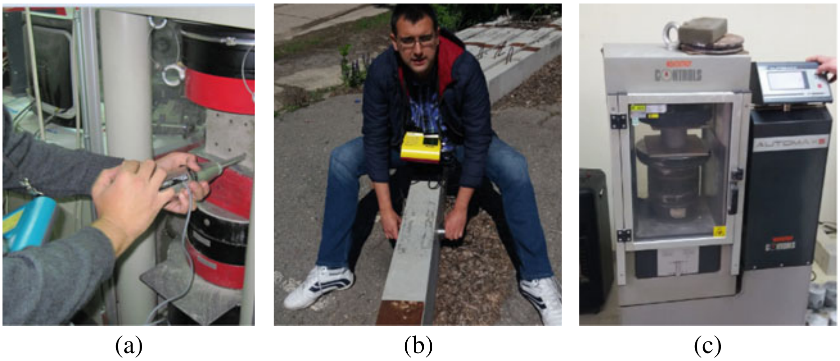


Fig. 2 Determining the rebound number (**a**); ultrasonic signal velocity (**b**); compressive strength by destructive tests of specimens (**c**) (personal archive)

number *R* of the 10 hits for each test point was calculated. The rebound number varies in the range *R* = 45–52, i.e., the rebound number increases with age.

A portable Proceq TICO ultrasonic device was used for the experimental determination of the ultrasonic signal velocity (Fig. 2b). The operating frequency of the transmitter and receiver is 54 kHz, and the resolution is 0.1 μs. The surfaces of 12 cubic test specimens and the reinforced concrete beams are smooth. Ensuring good contact between the piezoelectric transducers and the concrete surfaces is done by a special coupling paste. For each test specimen, 10 measurements of the ultrasonic velocity were made according to EN 12504-4:2005. The transmitter and receiver of the ultrasonic device were located symmetrically against each other. Before each measurement, the equipment was calibrated with a reference cylindrical body with a known velocity.

Ultrasonic velocity measurements on age 1126th day were made on two opposite sides of the cubes, and measurements on age 1926th day were made on two opposite sides of the beams in places from which the cores would be taken. The value of UPV for age 1126th day is *V* = 4.335–4.442 km/s, and for the 1926th day, it is *V* = 4.578–4.876 km/s, i.e., the velocity of the ultrasonic signal increases with age.

The compressive strength of concrete from a test of 12 cubes with standard dimensions at age 1126th day was determined with destructive tests (Fig. 2c) according to EN 12390-3:2009. The test specimens were tested on compression till failure on a calibrated material testing machine type: 50-C4652 (0–2000) kN, CONTROLS Automax 5, corresponding to EN 12390-4:2001. A constant load rate of 0.5 MPa/s has been selected, according to the requirements of the EN 12390-3:2009 standard. The load is applied to the test specimen without hit and increases evenly until failure, the force F [kN] was recorded and compressive strength [N/mm^2] was calculated.

At age of concrete 1926th day, the drilled cores were tested on the same machine, and the compressive strength was determined by dividing the load at failure by the cross-sectional area of the core. The cores were taken from the members according to EN 12504–1:2019, and the compressive strength was determined according to EN

12390-3:2009. According to BDS EN 13791:2007/NA:2011, if the ratio of the height of the core L to the diameter D is equal to 1, the obtained compressive strength must be equal to the compressive strength of a cube with a side of 150 mm. Before testing the cores, their mass and geometric dimensions were determined. The compressive strength f_c for age 1126th day varies from 39.97 to 47.12 MPa and for the 1926th day varies from 42.4 to 52.5 MPa, i.e., it increases with age.

5 Analysis of Results. Models and Correlation Curves

Drawing of regression (correlation) curves from mathematical models for the dependences of the compressive strength of concrete obtained by the destructive method on the rebound number, on the ultrasonic velocity and on $f_{c,\mathrm{SonReb}}$ determined with the SonReb method were made with Excel. The obtained graphs show the approximating line, the equations of this line, and the value of the correlation coefficient R^2, by which the reliability of the approximation can be estimated. The closer its value is to 1, the more precisely the selected function approximates the data. For obtaining correlation curves between the results of concrete compressive strength obtained by destructive method, and the results of non-destructive tests the constants a, b, and c were determined in Eq. (1), using regression analysis in Microsoft Excel and $f_{c,\mathrm{SonReb}}$ was determined.

When creating empirical correlation formulas to study the effectiveness of the combination of non-destructive measurements with the destructive testing of test specimens, the coefficient R^2 was compared with the models obtained from those with non-destructive techniques separately.

Figures 3 and 4 show the dependences of the compressive strength of concrete, determined by a destructive test of cubes at age 1126 days and destructive test of cores at age 1926 days on the rebound number R and on the velocity of the ultrasonic

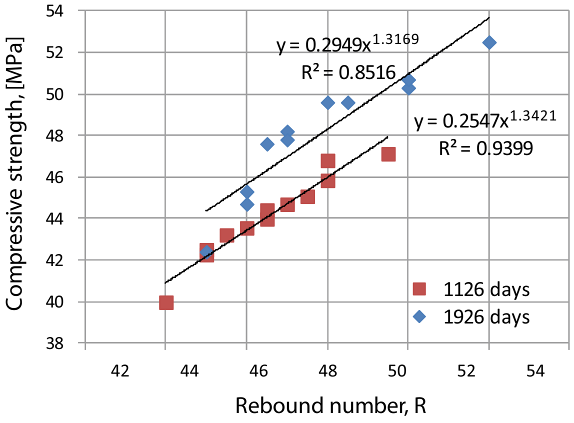
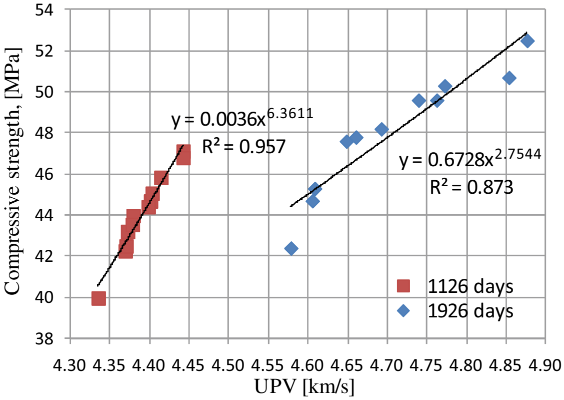


Fig. 3 Relationship of the concrete compressive strength, determined by destructive tests of specimens on the rebound number R at the age of 1126 and 1926 days

Fig. 4 Relationship of the concrete compressive strength, determined by destructive tests of specimens on the UPV at the age of 1126 and 1926 days



signal (UPV). The dependencies show that the magnitude of the rebound number and the UPV increases with increasing compressive strength, and the accuracy of the selected power equations have a very good correlation—the parameter R^2 is 0.940 and 0.957, respectively, at age of concrete 1126 days and the parameter R^2 is 0.852 and 0.873, respectively, at age of concrete 1926 days.

Figure 5 shows the dependence of the compressive strength determined by of the destructive test of cubes at age 1126 days and destructive test of cores at age 1926 days on the compressive strength determined by the SonReb method according to formula (1). The parameter $\mathrm{R}^2_{\mathrm{combined}}$ in the combined use of Schmidt hammer and UPVM for age 1126 days is equal to 0.9728, for age 1926 days is equal to 0.8824 (it is fulfilled that $R^2_{\mathrm{combined}} > R^2_{\mathrm{single}}$), i.e., the combination gives a more reliable estimate compared to the use of the two techniques separately.

For the specific experimental data on the compressive strength of concrete, determined by destructive testing of test specimens, on the magnitude of the rebound number R and on UPV at the age of 1126 days, Eq. (1) takes the form:

$$f_{c,\mathrm{SonReb}} = 0.0171 R^{0.5593} V^{3.8562} \tag{2}$$

Based on Eq. (2) with Excel, multiple regression curves were obtained to determine the compressive strength of concrete for the specific reinforced concrete structure (Fig. 6) [1, 15]. The resulting expression for $\mathrm{f}_{\mathrm{c,SonReb}}$ can be used to determine the compressive strength for any region of the existing reinforced concrete structure.

For the specific experimental data on the compressive strength of concrete, determined by destructive testing of test specimens, on the magnitude of the rebound number R and on UPV at the age of 1926 days, Eq. (1) takes the form:

$$f_{c,\mathrm{SonReb}} = 0.5003 R^{0.39} V^{1.9723} \tag{3}$$

Based on Eq. (3), multiple regression curves were obtained to determine the compressive strength for the specific reinforced concrete structure (Fig. 7) [1, 15].

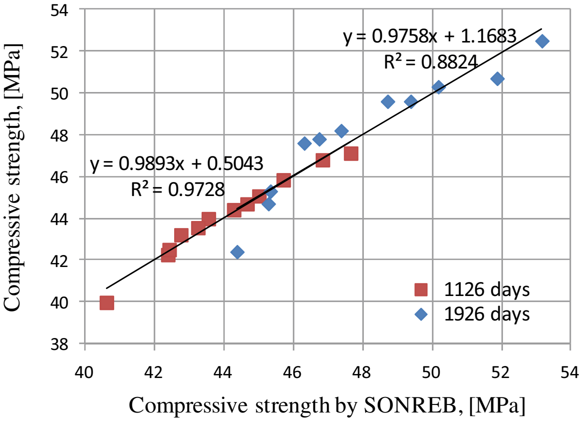


Fig. 5 Relationship of the compressive strength, determined by destructive tests of specimens on the compressive strength determined by SonReb at the age of 1126 and 1926 days

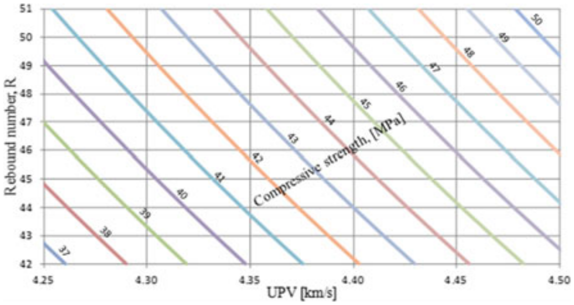


Fig. 6 Iso-strength curves for determining the compressive strength of concrete obtained by the SonReb method at the age of 1126 days

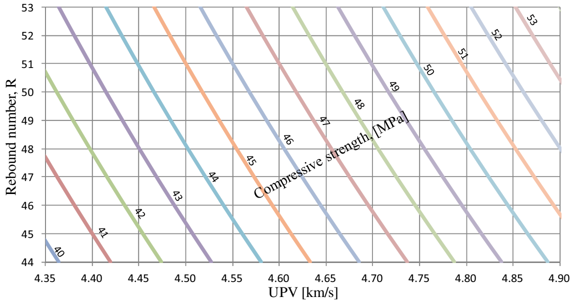


Fig. 7 Iso-strength curves for determining the compressive strength of concrete obtained by the SonReb method at the age of 1926 days

6 Conclusion

Based on the experimental studies and the developed models, the following conclusions can be made:

- The correlation coefficient R^2 of the proposed models for the dependence of the compressive strength of concrete f_c, determined by the destructive testing of specimens on the rebound number R varies from 0.852 to 0.94. The coefficient R^2 of the proposed models for the dependence of the compressive strength of concrete f_c, determined by the destructive testing of specimens on UPV varies from 0.873 to 0.957. This shows a good relationship between compressive strength, rebound number value, and UPV. Thus, rebound number and UPV are important predictors;

- Dependence on only one test method (rebound hammer test or ultrasonic pulse velocity test) does not always give sufficiently accurate results. In the developed correlation curves between the compressive strength of concrete f_c, determined by the destructive testing of specimens and the compressive strength determined by the method SonReb $f_{c,\mathrm{SonReb}}$, the correlation coefficient R^2 varies from 0.8824 to 0.9728. This shows the best relationship and greater accuracy between compressive strength and the combination of two non-destructive methods. The development of such dependencies helps for more accurate assess and track the characteristics of concrete over a long period of time;
- If for a reinforced concrete structure, we have results for compressive strength of concrete f_c, obtained from destructive testing of specimens, value of rebound number and velocity of the ultrasonic pulse. For a given number of test points, the value of compressive strength $f_{c,\mathrm{SonReb}}$ can be determined using correlation curves for any part of the structure. This allows to reduce the number of destructive tests of cores taken from existing reinforced concrete structures and to limit damage, using only the values of the rebound number and UPV for the whole structure.

From the experiments performed and the derived models for determining the compressive strength of concrete with the SonReb method, there is still no general consensus in the literature on the effectiveness of this combination, and this approach needs further research.

Acknowledgements This research was supported by the BG NSF Grant No KP-06-OPR01/3-2018 financed by the Ministry of Education and Science, Bulgaria.

References

1. Alwash M (2017) Assessment of concrete strength in existing structures using nondestructive tests and cores: analysis of current methodology and recommendations for more reliable assessment. Mechanics. Université de Bordeaux. NNT:2017BORD0587
2. Minutolo V et al (2019) The use of destructive and non-destructive testing in concrete strength assessment for a school building. IJARET 10(6):252–267. https://doi.org/10.34218/IJARET.10.6.2019.028
3. Jain A et al (2013) Combined use of non-destructive tests for assessment of strength of concrete in structure. Pr Eng 54:241–251. https://doi.org/10.1016/j.proeng.2013.03.022
4. Cristofaro M et al (2012) Mechanical characterization of concrete from existing buildings with SonReb method. 15 WCEE, Lisboa
5. Hannachi S, Guetteche M (2012) Application of the combined method for evaluating the compressive strength of concrete on site. Open J Civ Eng 2. https://doi.org/10.4236/ojce.2012.21003

6. Wang X, Jiang K (2016) Quality control and evaluation methods of concrete engineering and its reliability analysis. Int J Simul Syst Sci Technol 17. https://doi.org/10.5013/IJSSST.a.17.17.15
7. Nobile L, Bonagura M (2013) Accuracy of non-destructive evaluation of concrete compression strength. In: 12th ICSSNDT, Slovenia, pp 57–64
8. Zatar W (2014) Assessing the service life of corrosion-deteriorated reinforced concrete member highway bridges in West Virginia. Marshall University
9. Khan A (2002) Guidebook on non-destructive testing of concrete structures. IAEA, Training Course Series 17, Vienna
10. Karaiskos G et al (2015) Monitoring of concrete structures using the ultrasonic pulse velocity method. Smart Mat Struct 24 (11). https://doi.org/10.1088/0964-1726/24/11/113001
11. Lorenzi A at al (2007) Ultrasonic pulse velocity analysis in concrete specimens. IV Conf Panamericana de Ensayos No Destructivos, Buenos Aires
12. Naik T et al (2004) The ultrasonic pulse velocity method. Handbook on nondestructive testing of concrete. CRC Press, USA
13. Pucinotti R (2007) The use of multiple combined non destructive testing in the concrete strenght assessent: applications on laboratory specimens. 4th ICNDT, Crete, Greece
14. Chandak N, Kumavat H (2020) SonReb method for evaluation of compressive strength of concrete. In: IOP IOP conference series: materials science and engineering (MSE), vol 810, issue no 1. https://doi.org/10.1088/1757-899X/810/1/012071
15. Nikhil M et al (2015) The use of combined non destructive testing in the concrete strength assessment from laboratory specimens and existing buildings. Int J Curr Eng Sci Res (IJCESR) 2(5):55–59
16. Jedidi M (2018) Evaluation of the concrete quality using destructive and non-destructive tests. MOJ Civil Eng 4(4):219–223. https://doi.org/10.15406/mojce.2018.04.00095
17. Dauji S et al (2019) Conservative characteristic strength of concrete from nondestructive and partially destructive testing. J Asian Concr Fed 5(1):25–39. https://doi.org/10.18702/acf.2019.06.30.25

IU-AutoSVD++: An Item–User Features-Based Recommender System Using Contractive Autoencoder and Matrix Factorization

Abdelghani Azri, Adil Haddi, and Hakim Allali

Abstract Matrix factorization is a successful approach in recommender systems that is used largely to provide adequate recommendations to users. In the last years, many approaches based on deep learning, such as autoencoders, were used or combined with other methods to extract nonlinear relationships between items. But most of these models do not include user's information side in the rating process. In the present article, we have proposed a new model IU-AutoSVD++ combining the matrix factorization and the contractive autoencoder in order to include item features and user side information. Experiments results prove that our model performs better than many baselines models.

Keywords Recommender system · SVD · SVD++ · SVD++ · AutoSVD++ · Matrix factorization · Deep learning · Contractive autoencoder

1 Preliminaries

Let us define S_I a set of items i of size $m \in \mathbb{N}$: $S_I = \{i_1, i_2, ..., i_m\}$ and S_I a set of users u of size $n \in \mathbb{N}$: $S_U = \{i_1, i_2, ..., u_n\}$. The matrix represents the interaction between users and items called rating matrix R. It is defined as sparse matrix with n lines and m items: $R \in \mathbb{R}^{m \times n}$. The rating value r is often defined as an integer in the set : $\{1, 2, .., 5\}$. Let us also define an item features vector f_i: $f_i = \{f_1, .., f_x\}$ of size x and a user features vector $f_u = \{e_1, .., e_y\}$ of size y.

A. Azri (✉) · H. Allali
FST, LAVETE Laboratory, Hassan First University of Settat, Settat 26000, Morocco
e-mail: a.azri@uhp.ac.ma

H. Allali
e-mail: hakim.allali@uhp.ac.ma

A. Haddi
ENSA, LAVETE Laboratory, Hassan First University of Settat, Berrechid 26100, Morocco
e-mail: a.haddi@uhp.ac.ma

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_61

2 Introduction

With the exploration of data “Big Data” in many areas such as E-commerce, music and video streaming, it is hard to avoid recommendation systems these days. At companies from YouTube to Netflix to Spotify to Amazon and beyond, recommendations are helping customers to find relevant products and businesses sell more items or products. In general, a recommender system (RS) is a tool used to bring the user an adequate item such as products, books, movies and music that he might be interested in.

Many successful approaches are used to develop RS, namely collaborative filtering approach which uses user’s historical preferences over an item to propose new items that may interest this user. The notable methods used in the collaborative filtering are the methods based on matrix factorization especially after the success of the Netflix context such as SVD, SVD++ and NMF. Another method uses a probabilistic technique such as PMF.

Recently, many other methods use the deep learning techniques such as the autoencoder: autoSVD++ and AutoRec or such as the convolution neural network (CNN) which is used to extract visual features. Most of these methods are widely used to capture the interaction between users and items like SVD and its variants in Koren [3, 4], Koren et al. [5]. Some works recently studied the items features like autoSVD++ in [10]. But most of these approaches do not capture the user side of user features. In this work, we will first present some successful approaches using matrix factorization techniques such as SVD, SVD+++ and an approach based on autoencoder: autoSVD++ which used the item features in addition to the rating information. Then, we will present our approach which is an extension of the autoSVD++. Our approach is based on the SVD++ and used two versions of the contractive autoencoder applied, respectively, on item features and user features. Finally, we present the results of our experiments and the future work.

3 Related Work

Many approaches are developed last years. These approaches are based on matrix factorization or latent factors space models such as SVD, SVD++, and PMF. Other approaches are based on deep learning techniques such as autoSVD++.

3.1 SVD-Based Models

SVD The simplest version of matrix factorization through SVD is given by the Eq. (1):

$$\hat{r}_{ui} = q_i^{\mathsf{T}} p_u = \sum_{k=1}^{k} q_{ki} p_{uk} \tag{1}$$

Biased SVD It is a variant of SVD model obtained by adding an item bias and a user bias to Eq. 1:

$$\hat{r}_{ui} = q_i^{\mathsf{T}} p_u + \mu + b_i + b_u \tag{2}$$

SVD++ The SVD++ is an extension version of biased SVD obtained by adding a term representing the user's implicit feedback. The implicit feedback represents in general the tendencies of the user regarding some items. It can be captured using some statistics like clicks, page visiting or historical purchases. It can be represented by binary values so if the user rates an item we give 1 value; otherwise, the 0 value is assigned.

$$\hat{r}_{ui} = \mu + b_i + b_u + q_i^{\mathsf{T}} (p_u + \frac{\sum\limits_{j \in S(u)} y_j}{\sqrt{|S(u)|}}) \tag{3}$$

Probabilistic matrix factorization (PMF) is a matrix factorization technique similar to singular value decomposition, but it uses statistical probability theory rather than linear algebra. PMF is developed by Mnih and Salakhutdinov in [7]. The PMF model computes a low rank factorization of a ratings matrix R where $R = UV^{\top}$ for $U \in \mathbb{R}^{n \times k}$ and $V \in \mathbb{R}^{m \times k}$. U and V are user and item latent matrices and K is small; for most of our experiments, K was less than 10.

The PMF model assigns a normal prior with zero mean and K dimensional user-specific variance, $\sigma_u^2 I_K$, to the user latent matrix U and a similar distribution to the item latent matrix V. Each rating $r_{i,j}$ is then assigned a normal distribution centered on $U_i V_j^T$ with rating variance σ^2.

$U_i \sim \mathcal{N}(0, \sigma_u^2 I_K)$, $V_i \sim \mathcal{N}(0, \sigma_v^2 I_K)$, $r_{ij} | U, V \sim \mathcal{N}(U_i^{\top} V_j, \sigma^2)$

$$P(R|U, V, \sigma^2) = \prod_{i=1}^{M} \prod_{j=1}^{N} [\mathcal{N}(R_{ij} | U_i^{\top} V_j, \sigma^2)]^{I_{ij}} \tag{4}$$

where $\mathcal{N}(x|\mu, \sigma_u^2)$ is the probability density function of the Gaussian distribution with mean, μ and variance, σ_u^2 and I_{ij} is the indicator function as:

$$I_{ij} = \begin{cases} 1, & \text{if user } i \text{ has rated item } j \\ 0, & \text{otherwise.} \end{cases}$$

3.2 AutoSVD++

AutoSVD++ is a hybrid model proposed in Zhang et al. [10], and it extends the SVD++ model by adding item features extracted based on contractive autoencoder (CAE) model proposed by Rifai et al. [8].

4 Our Model

Our contribution aims to propose a new model called **IU-AutoSVD++** extending the autoSVD++ model proposed in [10] by adding user features which can express the user's profile. So first, we extracted the item and user features described in Table 1. First, let us introduce the autoencoder model and the CAE model.

4.1 Autoencoders

An autoencoder(AE) is an unsupervised artificial neural network, and it is appeared for the first time in [1]. It is composed of two parts: an encoder part and a second one called decoder. The main idea of a AE is to compute the input layer using the hidden layer: $h = f(x)$ in order to construct the output layer: $r = g(h)$. The AE is used in many areas: dimensional reduction, feature learning and object classification.

Many variants of the autoencoder were used recently in recommender systems [9] and [2]. In this work, we will use the contractive autoencoder (CAE) proposed in Rifai et al. [8].

4.2 Contractive Autoencoder

The contractive autoencoder(CAE) [8] is an autoencoder that aims to make the input robust regarding the small changes around the training points level by adding a penalty term to the usual reconstruction function.

Table 1 Item–user features

Element	Features
User	Age, gender, job
Item	Genre, Year of apparition

First the input is projected in a hidden latent space h as in Eq. (5):

$$h_i = \sigma(Wx + b_h) \tag{5}$$

Equation 6 computes the Jacobian of h with respect to the input x.

$$J_i = h_i(1 - h_i) * W_i \tag{6}$$

Then the CAE tries to reconstruct the output by computing the reconstruction of the given input Eq. (7):

$$y = \sigma(W'h + b_y) \tag{7}$$

where σ is the $sigmoid$ activation function : $\sigma(z) = \frac{1}{1+\exp(-z)}$.

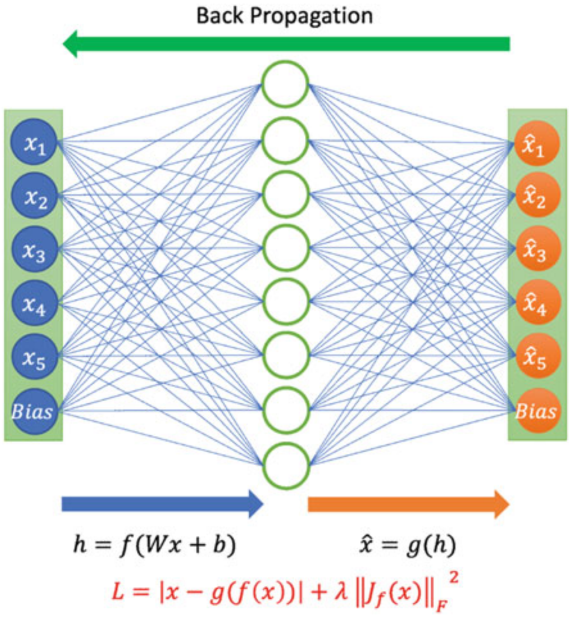
We suppose that $W^\intercal = W'$ as mentioned by authors in Rifai et al. [8].

The loss function used to learn the contractive autoencoder parameters $\{W, b_h, b_y\}$ is given by the Eq. (8):

$$L = \|X - \hat{X}\|_2^2 + \lambda \|J_h(X)\|_F^2 \tag{8}$$

The regulation term corresponds to the the Jacobian matrix in Frobenius norm $\| \|_F^2$ given by Eq. (9):

Fig. 1 Contractive autoencoder (CAE)



$$\|J_h(X)\|_F^2 = \sum_{ij} \left(\frac{\partial h_j(X)}{\partial X_i} \right)^2 \tag{9}$$

This regulation is calculated by summing the squares of all partial derivatives corresponding to the extracted features regarding the input dimensions (Fig. 1).

4.3 The IU-AutoSVD++ Model

IU-AutoSVD++ is a combination of three models:

(a) The model SVD++ model mentioned in Eq. (3);
(b) The I-CAE model applied on the item features followed by a linear transformation to reduce the vector item features dimension to the k corresponding of the latent space features equation (10);
(c) The U-CAE model applied on the vector user features with a linear transformation to reduce the feature dimension to the same latent space features k Eq. (11);

The item features vector is given by:

$$\text{CAE}(f_i) = \sigma(W.f_i + b) \tag{10}$$

The user features vector is given by:

$$\text{CAE}(f_u) = \sigma(W.f_u + b') \tag{11}$$

The item–user features are encoded as one hot encoded (0 or/and 1 values). Tables 2 and 3 represent, respectively, the item and user features matrices.

The next step is to apply CAE model [10] to extract compressed and useful representations of both item and user features. Then we run a linear transformation in order to have the same dimension space D which is equal to k the latent factors space. The results of this operation is represented in Tables 4 and 5, respectively.

The last step is to combine equations of SVD++ (3) , I-CAE(10), and U-CAE (11) in order to obtain Eq. (12) of our model:

Table 2 Encoded item features

Item id	f_1	f_2	f_3	...	f_{x-1}	f_x
item$_1$	0	0	1	□	1	0
item$_2$	1	1	0	□	0	1
...	□	□	□	□	□	□
item$_m$	1	0	0	□	1	1

Table 3 Encoded user features

User id	f_1	f_2	f_3	...	f_{y-1}	f_y
user$_1$	0	0	1	□	1	0
user$_2$	1	1	0	□	0	1
...	□	□	□	□	□	□
user$_n$	1	0	0	□	1	1

Table 4 Compressed item features

Item id	f_1	f_2	f_3	...	f_{k-1}	f_k
item$_1$	ω_{11}	ω_{12}	ω_{13}	□	ω_{1k-1}	ω_{1k}
item$_2$	ω_{21}	ω_{22}	ω_{23}	□	ω_{2k-1}	ω_{2k}
...	□	□	□	□	□	□
item$_m$	ω_{m1}	ω_{m2}	ω_{m3}	□	ω_{mk-1}	ω_{mk}

Table 5 Compressed user features

User id	f_1	f_2	f_3	...	f_{k-1}	f_k
user$_1$	ω'_{11}	ω'_{12}	ω'_{13}	...	ω'_{1k-1}	ω'_{1k}
user$_2$	ω'_{21}	ω'_{22}	ω'_{23}	...	ω'_{2k-1}	ω'_{Bk}
...	□	□	□	□	□	□
user$_n$	ω'_{n1}	ω'_{n2}	ω'_{n3}	...	ω'_{nk-1}	ω'_{nk}

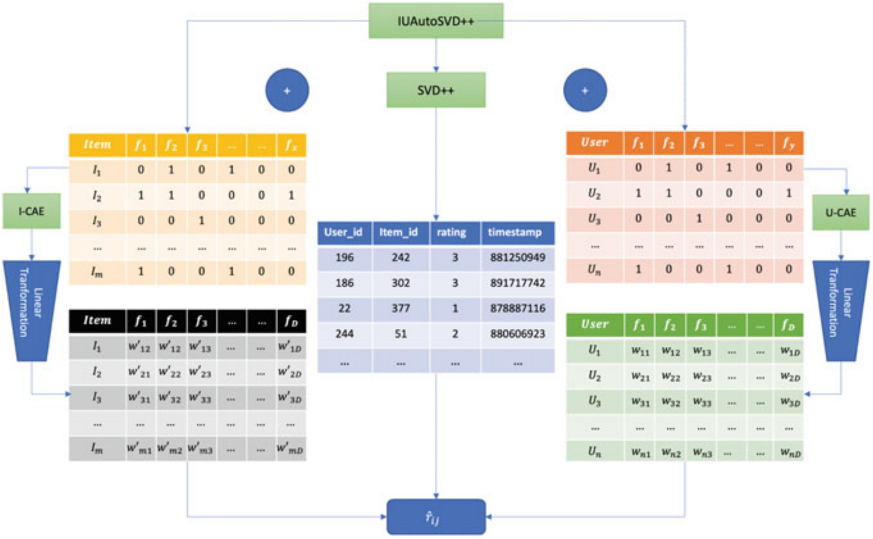
$$\hat{r}_{ui} = \mu + b_i + b_u + (\beta.CAE(f_i) + q_i)_i^{\mathsf{T}}(p_u + \theta.\text{CAE}(f_u) + \frac{\sum\limits_{j\in S(u)} y_j}{\sqrt{|S(u)|}}) \tag{12}$$

where $q_i \in \mathbb{R}^k(k = 1..m)$ is the item-based vector, $p_u \in \mathbb{R}^k(k = 1..n)$ is the user-based vector in the latent space, y_i is a vector representing the implicit feedback, and β and θ are parameters used to normalize CAE(f_i) and CAE(f_u), respectively. The whole architecture of our model is represented in Fig. 2.

4.4 Optimization

Equation 13 represents the loss function of our model:

$$\begin{aligned}\mathcal{L} &= \min \sum_{u,i\in K} [r_{ui} - (\beta.\text{CAE}(f_i) + q_i)^{\mathsf{T}}(p_u + \theta.\text{CAE}(f_u) + \frac{\sum\limits_{j\in S(u)} y_j}{\sqrt{|S(u)|}}) - \mu - b_u - b_i]^2 + \\ &\quad \lambda_y(b_u^2 + b_i^2 + \|p_u\|^2 + \|q_i\|^2 + \sum_{j\in S(u)} \|y_j\|^2)\end{aligned} \tag{13}$$



Item	f_1	f_2	f_3	...	...	f_x
I_1	0	1	0	1	0	0
I_2	1	1	0	0	0	1
I_3	0	0	1	0	0	0
...	...	...	...	...	...	...
I_m	1	0	0	1	0	0

Item	f_1	f_2	f_3	...	...	f_D
I_1	w'_{12}	w'_{12}	w'_{13}	...	...	w'_{1D}
I_2	w'_{21}	w'_{22}	w'_{23}	...	...	w'_{2D}
I_3	w'_{31}	w'_{32}	w'_{33}	...	...	w'_{3D}
...	...	...	...	...	...	...
I_m	w'_{m1}	w'_{m2}	w'_{m3}	...	...	w'_{mD}

User_id	Item_id	rating	timestamp
196	242	3	881250949
186	302	3	891717742
22	377	1	878887116
244	51	2	880606923
...	...	...	...

User	f_1	f_2	f_3	...	...	f_y
U_1	0	1	0	1	0	0
U_2	1	1	0	0	0	1
U_3	0	0	1	0	0	0
...	...	...	...	...	...	...
U_n	1	0	0	1	0	0

User	f_1	f_2	f_3	...	...	f_D
U_1	w_{11}	w_{12}	w_{13}	...	...	w_{1D}
U_2	w_{21}	w_{22}	w_{23}	...	...	w_{2D}
U_3	w_{31}	w_{32}	w_{33}	...	...	w_{3D}
...	...	...	...	...	...	...
U_n	w_{n1}	w_{n2}	w_{n3}	...	...	w_{nD}

Fig. 2 IU-AutoSVD++ model

where λ_y is a regulation factor that is determined during the training the model.

In order to learn the parameters corresponding to the model, we use the stochastic gradient descent (SGD) algorithm. The SGD calculates a single prediction r_{ui} and its error in Eq. (14) as follows:

$$\text{error}_{ui}^2 = (r_{ui} - \hat{r}_{ui})^2 \tag{14}$$

5 Experiments

In this section, we present the datasets used to run the experiments, the evaluation metric and the experiments results as follows:

5.1 *Datasets*

In order to evaluate our model, we conduct many experiments on two public datasets provided by MovieLens site which are largely used in the recommender systems area. The characteristics of both datasets are presented in Table 6 as follows:

Table 6 MovieLens datasets

Dataset	Number of items	Number of users	Number of ratings	Density (%)
100K	1682	943	100000	6.30
1M	6040	3706	1000209	4.47

5.2 Model Evaluation Metric

The root mean square error (RMSE) metric is used to evaluate our model. The formula of the RMSE is given by Eq. (15) as follows:

$$\text{RMSE} = \sqrt{\frac{1}{|\hat{R}|} \sum_{\hat{r}_{ui} \in \hat{\mathbf{R}}} (r_{ui} - \hat{r}_{ui})^2} \tag{15}$$

where R denotes the rating matrix.

5.3 Results and Discussions

We have compared our model with the following baseline models:

1. Biased SVD: A basic version of matrix factorization with user and item bias proposed in [5]
2. SVD++: An extended version of the matrix factorization which include the implicit feedback [5]
3. NMF: A collaborative filtering algorithm based on non-negative matrix factorization [6]. It is a model similar to the SVD model. The idea of NMF model is to keep user and item factors positive.
4. PMF: The model proposed in [7]
5. autoSVD++: A model proposed by Zhang et al. [10].

Table 7 shows the experimental results of our model compared with other baseline models.

The results prove that our model performs better than the compared baseline models for both $100K$ and $1M$ datasets.

Table 7 RMSE experiments results for 100K and 1M MovieLens datasets

Model	ML-100K (RMSE)	ML-1M(RMSE)
SVD	0.934	0.873
SVD++	0.913	0.855
PMF	0.952	0.883
NMF	0.952	0.883
AutoSVD++	0.904	0.848
IU-AutoSVD++ (our model)	**0.896**	**0.846**

Bold highlights our model and the corresponding results

6 Conclusion

We have proposed a new hybrid model IU-AutoSVD++ by adding both the item features and the user side information. Our model integrates item and user side information which seems to be helpful improving the prediction's accuracy. One of the limitations in our model is that it is still static and does not include other rich information such as item image or description. So many extensions are possible in the future to make it more efficient and accurate as follows:

- Add other rich contents such as visual features of item to extract more relationships and improve the prediction.
- Since the rating process is not static and may change over the time, including the time factor will bring efficiency to the model.
- Run more experiments on other datasets.
- Experiment other metrics to evaluate and compare the results of our model with other existing models.

References

1. Ballard DH (1987) Modular learning in neural networks. In: Forbus K, Shrobe H (eds) Proceedings of the sixth national conference on artificial intelligence, pp 279–284. Morgan Kaufmann, San Francisco, CA. http://www.mpi-sb.mpg.de/services/library/proceedings/contents/aaai87.html
2. Bank D, Koenigstein N, Giryes R (2021) Autoencoders. arXiv:2003.05991 [cs, stat] (Apr 2021), http://arxiv.org/abs/2003.05991, arXiv: 2003.05991
3. Koren Y (2008) Factorization meets the neighborhood: a multifaceted collaborative filtering model. In: Li Y, Liu B, Sarawagi S (eds) Proceedings of the 14th ACM SIGKDD international conference on knowledge discovery and data mining, Las Vegas, Nevada, August 24–27, pp 426–434. ACM. https://doi.org/10.1145/1401890.1401944
4. Bell RM, Koren Y, Volinsky C (2009) The bellkor solution to the netflix grand prize. AT&T Labs. https://www.bibsonomy.org/bibtex/24e6c6e6bcc4d825e9f2a6ac98bbab56a/dhruvbansal

5. Koren Y, Bell R, Volinsky C (2009) Matrix factorization techniques for recommender systems. Computer 42(8):30-37 (2009). https://doi.org/10.1109/MC.2009.263. http://ieeexplore.ieee.org/document/5197422/
6. Lee D, Seung HS (2001) Algorithms for non-negative matrix factorization. In: Leen T, Dietterich T, Tresp V (eds) Advances in neural information processing systems, vol 13. MIT Press (2001). https://proceedings.neurips.cc/paper/2000/file/f9d1152547c0bde01830b7e8bd60024c-Paper.pdf
7. Mnih A, Salakhutdinov RR (2008) Probabilistic matrix factorization. In: Platt JC, Koller D, Singer Y, Roweis ST (eds) Advances in neural information processing systems vol 20, pp 1257–1264. Curran Associates, Inc. http://papers.nips.cc/paper/3208-probabilistic-matrix-factorization.pdf
8. Rifai S, Vincent P, Muller X, Glorot X, Bengio Y (2011) Contractive auto-encoders: explicit invariance during feature extraction. In: Getoor L, Scheffer T (eds) ICML. Omnipress, pp 833–840. http://dblp.uni-trier.de/db/conf/icml/icml2011.html#RifaiVMGB11. https://www.bibsonomy.org/bibtex/28f26a7044285547aa837507603c30b77/dblp
9. Schmidhuber J (2015) Deep learning in neural networks: an overview. Neural Netw 61:85–117 (2015). https://doi.org/10.1016/j.neunet.2014.09.003. http://arxiv.org/abs/1404.7828, arXiv: 1404.7828
10. Zhang S, Yao L, Xu X (2017, August) AutoSVD++: an efficient hybrid collaborative filtering model via contractive auto-encoders. In: Proceedings of the 40th international ACM SIGIR conference on research and development in information retrieval, pp 957–960. https://doi.org/10.1145/3077136.3080689. http://arxiv.org/abs/1704.00551, arXiv: 1704.00551

Model Learning and Tactical Maneuver Planning for Automatic Driving

Micha Helbig, Jens Hoedt, and Ulrich Konigorski

Abstract Tactical maneuver planning is one of the key enablers for automated driving. The challenges include complex situations in urban areas and the uncertain behavior of other road users. In this paper, we present an approach to model the decision problem of tactical maneuver planning as a Markov decision process (MDP) for a two-lane road. It is shown how this model can be used to make tactical maneuver decisions on a three-lane road without increasing the complexity of the MDP. Furthermore, it is shown how the model can be learned and improved in a three-lane simulation environment using real-world experience. The results show that the learned model represents the environment better than the manually modeled MDP and that a significantly better driving strategy is calculated based on this.

Keywords Automated driving · Tactical maneuver planning · Markov decision process · Model learning

1 Introduction

Automatic driving has the potential to improve the way we travel in many different ways. Today, driver assistance systems already relieve the driver of many tasks. Systems such as emergency lane assist or lane-keeping assist have helped to reduce accidents on roads in the last years. However, still 88.5% of accidents in 2020 could be attributed to human error on the part of vehicle drivers in Germany [16]. The number of these accidents can be significantly reduced by automatic driving functions. Fur-

The results, opinions and conclusions expressed in this thesis are not necessarily those of Volkswagen Aktiengesellschaft.

M. Helbig (✉) · J. Hoedt
Volkswagen AG, Wolfsburg, Germany
e-mail: micha.helbig@volkswagen.de

U. Konigorski
Technische Universität Darmstadt, Darmstadt, Germany

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_62

thermore, efficient route planning and anticipatory driving behavior of automatically driving cars have the potential to reduce fuel consumption and thus also emissions of climate-damaging greenhouse gases. In addition to safety and environmental aspects, comfort for the driver and for passengers can also be improved. Fully autonomous vehicles would no longer need a driver, allowing people to occupy themselves with other activities in the vehicle.

Therefore, the development of new technologies for automated driving has attracted increasing interest from the scientific community as well as industry over the past two decades. A major leap was made in the 2007 Darpa Urban Challenge, in which scientists from around the world competed to develop a vehicle that could autonomously navigate through an urban area, avoid obstacles, and obey traffic rules [3]. This goal poses many challenges. Therefore, the driving task is usually hierarchically divided into four components, namely the route planning, behavioral decisions, local motion planning, and feedback control [14]. The behavioral decision layer, also called tactical maneuver planning, makes high-level decisions about how the car should behave on a road with traffic rules and other road users. Should the car change lanes and overtake the vehicle in front or should it stay in the lane because it has to turn at the next intersection? The driving task is to guide the vehicle through a multi-lane road in a collision-free, time-efficient, and comfortable way. To do this, the car can choose from several high-level actions. These include accelerating, maintaining speed, braking, and changing lanes. Based on this planning, the local motion planning calculates an exact path that can be controlled by the feedback control.

Tactical maneuver planning for automated driving is particularly complex in urban areas, as it depends on a number of different influences such as other road users, multilane roads, or traffic lights. In the Darpa Challenge, finite state machines were the most commonly used approaches to tackle this challenge [3]. However, due to the many different possible situations and the dynamic and stochastic environment, it is difficult to find safe and time-efficient maneuvers with rule-based methods.

Another approach is to model a Markov decision process (MDP) and compute a driving policy based on it. To account for the stochastic behavior of other road users and the simplicity of the model, we learn the transition model of the MDP to obtain a more accurate model. We achieve this by adding transitions and updating transition probabilities from experience gained in a simulation environment. Lopez et al. [1] refer to this as active learning of MDP models. This model can then be examined in detail so that assessments can be made about the quality of the model. This learning process could also be done with data from real sensor measurements. With this method, we can achieve much more accuracy and a better driving behavior.

The work is organized as follows: In Sect. 2, we give an overview of the state of the art. In Sect. 3, we show how the initial MDP is modeled and a driving strategy is generated based on it. Then we show how the MDP can be learned in a simulation environment and the new driving strategy can be applied to three-lane roads. The simulation environment and setup are described in Sect. 5. We present and discuss the results in Sects. 6 and 7. Finally, Sect. 8 summarizes the work and gives an outlook on future work.

2 Related Work

Guan et al. [6] model an MDP for a two-lane road with an ego vehicle and one additional vehicle. They use statistical data to predict the driving behavior of the other road user and model a stochastic transition model based on this data using the Monte Carlo method. Brechtel et al. [2] also use the Monte Carlo method to compute a transition model for their MDP. However, they do not compute a solution for the entire state space offline, but use a combination of an online and offline planner. This initializes just a few states of the MDP offline, for which a driving strategy is computed. Afterward, the states experienced in real time are added to the state space and a driving strategy is calculated locally for them. The idea is a trade-off between the online and offline computation time and the fact that the planner usually plans near the actual executed path. Due to the hybrid approach, however, calculations for different states take different amounts of time, so that either powerful hardware is still required or a good solution cannot be found in every state. Since with our approach the solution for the entire defined state space is already computed offline and the action only needs to be obtained from a table, our approach does not require powerful hardware for online planning in the vehicle and delivers a solution with a constant time requirement in every defined state.

Also, partial observable Markov decision processes (POMDP) are used. Ulbrich and Maurer [19] model a POMDP to incorporate sensor inaccuracies into the lane change decision and evaluate their approach in real traffic. Liu et al. [11] integrate the road context, the driver and the motion intention of another vehicle in the POMDP. Hubmann et al. [9] reduce the dimensionality of the problem by planning the vehicle motion on predefined paths. Nevertheless, these approaches remain computationally expensive and must be solved online because POMDPs are even more complex than MDPs. In addition, the uncertain behavior of other road users is modeled in a fixed way and the model is not improved by experience.

Our work is also related to reinforcement learning approaches as the theory is also based on the Bellman equation and MDPs [18]. Hoel et al. [7, 8] train a convolutional neural network to make decisions about lane changes and speed changes. However, due to the black-box nature of neural networks, no safe actions can be guaranteed. Krasowski et al. [10] address this problem by incorporating a safety layer that only allows safe actions. In contrast, we use a table-based approach with a model of the environment. This makes the decision-making process completely transparent. Therefore, the driving policy can be examined in detail before it is used in a real vehicle and thus eliminates the need for an additional safety layer during operation. Since tactical maneuver planning and autonomous driving is a very active field of research, there are many other approaches that cannot be described in detail here. For a more in-depth consideration, we suggest the works of Schwarting et al. [15] and Claussmann et al. [4].

The authors are not aware of approaches for tactical maneuver planning in which an MDP is learned based on experience in simulation. However, Lopez et al. [1] describe in general how the transition model of an MDP can be specifically learned by applying Bayesian reinforcement learning as an exploration strategy. In this way, state space regions are targeted in which the model has gained little experience before. In model-based reinforcement learning, models can be used to learn as much as possible from little experience. Sutton [17] introduced the Dyna algorithm, in which a model and a policy are simultaneously learned. The model in this case generates additional simulated experiences that the reinforcement learning algorithm uses to optimize the policy. For further insight into model-based reinforcement learning, we suggest the work of Moerland et al. [13].

3 Modeling the MDP

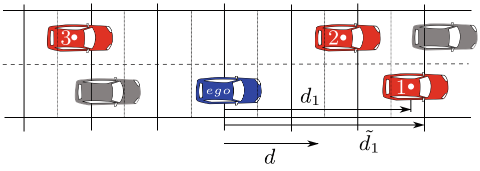
In this section, the driving task for a two-lane road is modeled as a deterministic MDP. On this basis, a driving strategy can be calculated using dynamic programming. Afterward, it is shown how this solution can be transferred to a three-lane roadway using a symmetry consideration without adapting the MDP and thus increasing the complexity. Finally, it is shown how the model can be improved with the help of experience from the simulation.

3.1 Environment Model

State Space The state vector should contain all variables that are necessary for decision making. However, with the number of variables the state space grows exponentially, and thus, the memory requirements and computation time. Therefore, only variables that have a high impact on decision making are used.

We use a curvilinear coordinate system, where we do not consider curvature. The most important variable is the ego velocity $v_{\text{ego}} \in \mathbb{R}$, since it is directly included in the reward function in Eq. 15. In order to be able to detect and prevent imminent collisions during a lane change, three other vehicles must also be considered: The front vehicle (vehicle 1) on the same lane and the front and rear vehicle (vehicle 2 and vehicle 3) on the adjacent lane (Fig. 1). Throughout the paper, we use the index $i \in \{1, 2, 3\}$ for variables to refer to vehicles 1, 2, and 3. For each of these vehicles, we consider the relative positions $d_i \in \mathbb{R}$ and the relative velocities $v_i \in \mathbb{R}$ to the ego vehicle, where $v_i = \dot{d}_i$.

Fig. 1 Two-lane state space for the MDP



For the representation of the environment as MDP, a finite discrete state space is required. For this purpose, the relative positions and velocities are mapped to the discrete sets $\tilde{D}_i$ and $\tilde{V}_i$, where $d_{i,\text{min}}$, $d_{i,\text{max}}$, $v_{i,\text{min}}$, and $v_{i,\text{max}}$ are the minimum and maximum relative distances and velocities and $G_{i,\text{d}}$, $G_{i,\text{v}} \in \mathbb{N}$ define the granularity of discretization with respect to the distance and velocity:

$$\tilde{D}_i := \{d_{i,\text{min}} + m\frac{d_{i,\text{max}} - d_{i,\text{min}}}{G_{i,\text{d}}} \mid m \in \mathbb{N}_0,\ m \leq G_{i,\text{d}}\} \tag{1}$$

$$\tilde{V}_i := \{v_{i,\text{min}} + m\frac{v_{i,\text{max}} - v_{i,\text{min}}}{G_{i,\text{v}}} \mid m \in \mathbb{N}_0,\ m \leq G_{i,\text{v}}\}\,. \tag{2}$$

Here, the elements $\tilde{v}_1 \in \tilde{V}_1$ and $\tilde{v}_2 \in \tilde{V}_2$ are predominantly negative and $\tilde{v}_3 \in \tilde{V}_3$ is predominantly positive, since in these ranges the distance of the respective vehicle to the ego vehicle is reduced after the next state transition and the vehicle thus has a higher impact on the decision making of the ego vehicle. For example, a slower vehicle 3 traveling at a safe distance behind the ego vehicle has little effect on a lane change decision, no matter how much slower it is. These states are summarized by the smallest element of the set $\tilde{V}_3$. On the other hand, this also models states in which the other vehicles are traveling outside the speed range of the ego vehicle. If, for example, the ego vehicle is driving with its maximum velocity and thus the maximum permissible speed and vehicle 3 overtakes with a higher velocity, these states are also modeled in the MDP until the maximum relative velocity is reached.

Equations 3 and 4 map the continuous d_i and v_i to the elements of the sets $\tilde{d}_i \in \tilde{D}_i$ and $\tilde{v}_i \in \tilde{V}_i$:

$$\tilde{d}_i = \begin{cases} d_{i,\text{min}}, & d_i \leq d_{i,\text{min}} \\ d_{i,\text{min}} + \\ \lfloor \frac{G_{i,\text{d}}(d_i - d_{i,\text{min}})}{d_{i,\text{max}} - d_{i,\text{min}}} + \frac{1}{2} \rfloor \frac{d_{i,\text{max}} - d_{i,\text{min}}}{G_{i,\text{d}}}, & d_{i,\text{min}} < d_i < d_{i,\text{max}} \\ d_{i,\text{max}}, & d_i \geq d_{i,\text{max}} \end{cases} \tag{3}$$

$$\tilde{v}_i = \begin{cases} v_{i,\text{min}}, & v_i \leq v_{i,\text{min}} \\ v_{i,\text{min}} + \\ \lfloor \frac{G_{i,\text{v}}(v_i - v_{i,\text{min}})}{v_{i,\text{max}} - v_{i,\text{min}}} + \frac{1}{2} \rfloor \frac{v_{i,\text{max}} - v_{i,\text{min}}}{G_{i,\text{v}}}, & v_{i,\text{min}} < v_i < v_{i,\text{max}} \\ v_{i,\text{max}}, & v_i \geq v_{i,\text{max}} \end{cases} \tag{4}$$

The granularity should be as coarse as possible and as fine-meshed as necessary to get a computationally feasible solution on one side and an accurate one on the other.

For each lane, the corresponding vehicle information can be aggregated. Hence, the state space for the lane of the ego vehicle is defined as:

$$
\begin{aligned}
\mathcal{S}_{\text{MDP}}^{\text{ego}} &: = \tilde{V}_{\text{ego}} \times \tilde{V}_1 \times \tilde{D}_1 && (5)\\
&= \{(\tilde{v}_{\text{ego}}, \tilde{v}_1, \tilde{d}_1) \mid \tilde{v}_{\text{ego}} \in \tilde{V}_{\text{ego}}, \tilde{v}_1 \in \tilde{V}_1,\ \tilde{d}_1 \in \tilde{D}_1\}\,. && (6)
\end{aligned}
$$

The state space of the adjacent lane is:

$$
\begin{aligned}
\mathcal{S}_{\text{MDP}}^{\text{adj}} &:= \tilde{D}_2 \times \tilde{V}_2 \times \tilde{D}_3 \times \tilde{D}_3 && (7)\\
&= \{(\tilde{v}_2, \tilde{v}_3, \tilde{d}_2, \tilde{d}_3) \mid \tilde{d}_2 \in \tilde{D}_2, \tilde{v}_2 \in \tilde{V}_2, && (8)\\
&\quad \tilde{d}_3 \in \tilde{D}_3, \tilde{v}_3 \in \tilde{V}_3\}\,. && (9)
\end{aligned}
$$

The state space is divided into this way in order to compose them modularly in Sect. 3.1 for the three-lane scenario. However, for the MDP, only the two-lane scenario is considered to keep the state space in a feasable size. The state space for this is given by $\mathcal{S}_{\text{MDP}} := \mathcal{S}_{\text{MDP}}^{\text{ego}} \times \mathcal{S}_{\text{MDP}}^{\text{adj}}$. **Action Space** An action is defined as a tuple $a = (\dot{v}, \delta_{\text{lc}}) \in \mathcal{A}_{\text{MDP}}$, where $\dot{v}$ is the longitudinal acceleration and $\delta_{\text{lc}} \in \{0, 1\}$ indicates, whether the ego vehicle changes its lane. $\mathcal{A}_{\text{MDP}}$ is the action space for the two-lane scenario. The ego vehicle can accelerate, maintain its velocity, brake or make a lane change. The action space $\mathcal{A}_{\text{MDP}}$ thus results to

$$
\mathcal{A}_{\text{MDP}} = \{ \underbrace{a_{\text{ac}}}_{\text{accelerate}}, \underbrace{a_{\text{st}}}_{\text{stay}}, \underbrace{a_{\text{br}}}_{\text{brake}}, \underbrace{a_{\text{lc}}}_{\text{lane change}} \}\,. \tag{10}
$$

In the MDP, we do not consider the two lanes as a left and a right lane, but as a lane on which the ego vehicle and vehicle 1 are located and a second lane on which vehicles 2 and 3 are located. It is irrelevant whether the second lane is on the left or on the right of the ego vehicle. After a lane change, these two lanes are swapped and the previous adjacent lane becomes the new ego lane.

Transition Model The transition model $p(s, a, s')$ states the probability of a transition from one state $s \in S_{\text{MDP}}$ to a next state $s' \in S_{\text{MDP}}$ for a given action $a \in A_{\text{MDP}}$. To keep the modeling simple, we model only one deterministic state transition with $p(s'|s, a) \in \{0, 1\}$ for each state $s \in S_{\text{MDP}}$. In further work, we plan to investigate also stochastic transitions. Furthermore, we assume that the participating vehicles maintain a constant speed and do not change lanes. The ego velocity v'_{ego}, the relative positions d'_i, and velocities v'_i after the transition can be calculated with the point-mass model:

$$
\begin{aligned}
v'_{\text{ego}} &= \tilde{v}_{\text{ego}} + t\dot{v}_{\text{ego}} && (11)\\
v'_i &= \tilde{v}_i - t\dot{v}_{\text{ego}} && (12)\\
d'_i &= \tilde{d}_i + \tilde{v}_i t - \frac{1}{2}\dot{v}_{\text{ego}} t^2\,, && (13)
\end{aligned}
$$

Before d'_i and v'_i are quantized with Eqs. 3 and 4 and assembled to the subsequent state, the effects of lane changes of the ego vehicle and overtaking maneuvers on the state have to be considered. Lane Change of the Ego Vehicle

A lane change can happen, if no vehicle in the state space overtakes during the transition. This case occurs if $d'_1 > 0$, $d'_2 > 0$ and $d'_3 < 0$. The arrangement of the vehicles in the state vector is then changed. Former vehicle 1 becomes vehicle 2 and former vehicle 2 becomes vehicle 1. Therefore, the indices for the relative positions d'_1, d'_2 and for the relative velocities v'_1, v'_2 are swapped. After a lane change, previous vehicle 3 would be located behind the ego vehicle, which is no longer represented in the model. A vehicle, which was behind the ego vehicle in the previous step, would now appear in the state space as vehicle 3. In the deterministic MDP, this vehicle is modeled as having minimum speed and relative position so that it does not affect the decision making in the next step. Overtaking Maneuvers

Another case is overtaking maneuvers from the ego vehicle or vehicle 3. If the ego vehicle does not make a lane change and the ego vehicle overtakes vehicle 2, so that $d'_2 < 0$, former vehicle 2 becomes vehicle 3 and vehicle 2 is modeled with the maximum relative position and velocity to the ego vehicle. In the opposite case $d'_3 > 0$, vehicle 3 overtakes the ego vehicle and vehicle 3 becomes vehicle 2, and vehicle 3 is modeled with the maximum relative position and velocity to the ego vehicle. Collision

Collisions are detected when the distance between the ego vehicle and another vehicle becomes smaller than the car length. In cases where the ego vehicle does not change lanes, only the distance d'_1 to vehicle 1 is considered. In the case of a lane change, the distances d'_2 and d'_3 are also considered. With the length of a car l_{car} a collision τ can thus be detected as follows:

$$\tau = \begin{cases} \text{true} & \text{if } d'_1 < l_{\text{car}} \\ \text{true} & \text{if } (d'_2 < l_{\text{car}} \text{ or } d'_3 > -l_{\text{car}}) \text{ and } \delta_{\text{lc}} = 1 \\ \text{false} & \text{else} \end{cases} \tag{14}$$

Although more than one collision can happen in the same transition, only one is considered.

Reward Model The vehicle should handle traffic in a time-efficient, comfortable, and collision-free manner. To achieve this, at each time step the velocity is rewarded with R_{v}. To ensure comfort, the vehicle should also make as few lane changes as possible. Therefore staying in lane is rewarded by a small positive reward R_{lc}. Finally, penalizing collisions with R_{c} ensures that the vehicle only learns safe maneuvers. In this case, no other rewards are given. The reward function is thus as follows (Fig. 2):

$$R = \begin{cases} R_{\text{v}} + R_{\text{lc}} & \text{if } \tau = \text{false} \\ R_{\text{c}} & \text{if } \tau = \text{true} \end{cases} \tag{15}$$

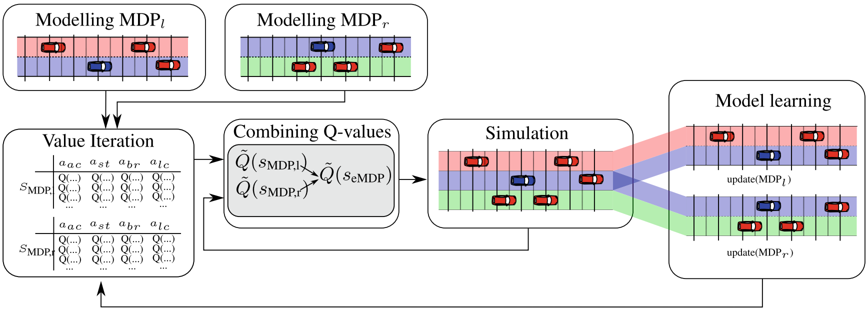


Fig. 2 Overview of the model learning process

Combining State Spaces Value iteration can now be used to calculate the Q-values for the respective actions in the MDP. These are stored in a table with the size $|S_{\text{MDP}} \times A_{\text{MDP}}|$ and can be used directly for decision making on the two-lane roadway. The extended state space for the three-lane case is then given by $S_{\text{eMDP}} = S^{\text{ego}}_{\text{MDP}} \times S^{\text{adj}}_{\text{MDP}} \times S^{\text{adj}}_{\text{MDP}}$, where an element of the set is denoted by $s_{\text{eMDP}} = (s^{\text{ego}}_{\text{MDP}}, s^{\text{adj,r}}_{\text{MDP}}, s^{\text{adj,l}}_{\text{MDP}}) \in S_{\text{eMDP}}$. The index adj,l represents the adjacent left lane and the index adj,r represents the adjacent right lane. The action space must also be extended so that lane changes can be displayed in both directions:

$$\mathcal{A}_{\text{eMDP}} = \{ \underbrace{a_{\text{ac}}}_{\text{accelerate}}, \underbrace{a_{\text{st}}}_{\text{stay}}, \underbrace{a_{\text{br}}}_{\text{brake}}, \underbrace{a_{\text{lc,l}}}_{\text{lane change left}}, \underbrace{a_{\text{lc,r}}}_{\text{lane change right}} \}. \tag{16}$$

Assuming that the left lane is irrelevant for a lane change decision to the right and in the opposite case the right lane is irrelevant for a lane change decision to the left, the symmetry of the problem can be exploited for planning on a three-lane roadway. The table for the two-lane road can be evaluated on both sides, for the center and right lanes as well as for the center and left lanes. We denote the longitudinal actions as $\mathcal{A}_{\text{lon}} = \{a_{\text{ac}}, a_{\text{st}}, a_{\text{br}}\} \subset \mathcal{A}_{\text{eMDP}}$. The Q-values of both tables are then combined for the extended state space S_{eMDP} and approximated as $\tilde{Q}_{\text{C}}$ as follows:

$$\begin{aligned} \tilde{Q}(s_{\text{eMDP}}, a_{\text{eMDP}}) &\approx \tilde{Q}_C(s^{\text{ego}}_{\text{MDP}}, s^{\text{adj}}_{\text{MDP, r}}, s^{\text{adj}}_{\text{MDP,l}}, a_{\text{eMDP}}) \\ &\approx \begin{cases} \max(\tilde{Q}(s^{\text{ego}}_{\text{MDP}}, s^{\text{adj}}_{\text{MDP,r}}, a_{\text{eMDP}}), \\ \qquad \tilde{Q}(s^{\text{ego}}_{\text{MDP}}, s^{\text{adj}}_{\text{MDP, l}}, a_{\text{eMDP}})) & \text{if } a_{\text{eMDP}} \in \mathcal{A}_{\text{lon}} \\ \tilde{Q}((s^{\text{ego}}_{\text{MDP}}, s^{\text{adj}}_{\text{MDP},r}), a_{\text{eMDP}}) & \text{if } a_{\text{eMDP}} = a_{\text{lc,r}} \\ \tilde{Q}((s^{\text{ego}}_{\text{MDP}}, s^{\text{adj}}_{\text{MDP},l}), a_{\text{eMDP}}) & \text{if } a_{\text{eMDP}} = a_{\text{lc,l}} \end{cases} \end{aligned} \tag{17}$$

In the first case, the maximum action value of the left and right table is taken for non lane change actions. The second and third cases are each evaluated only once by the corresponding table for the left and right action. Since the action values are not evaluated on S_{MDP} and A_{MDP}, but on S_{eMDP} and A_{eMDP}, Q_{C} is only an approximation to the real action values. However, this makes it possible to significantly reduce the state space for the three-lane road. Assuming that $\tilde{V} = \tilde{D} = N$, then the complexity would be $\mathcal{O}_{\text{MDP}}(N^7) \ll \mathcal{O}_{\text{eMDP}}(N^{11})$.

4 Model Learning

The deterministic MDP described so far assigns only one subsequent state to each state-action pair. However, due to the quantization of the state space and the non-deterministic behavior of the other road users, it does not adequately represent the real environment. For this reason, the MDP is learned with experience from the simulation.

Therefore, we approximate the probabilities with the relative frequencies $h(s'|s, a)$:

$$p(s, a, s') \approx h(s'|s, a) \tag{18}$$

Each state-action pair is now assigned a set of transitions $T_{s,a}$ that initially consists only of the transition described in Sect. 3.1 and thus $|T_{s,a}| = 1$.

We define a transition as $t_{s,a} = (s', n) \in T_{s,a}$, where s' is the subsequent state and n is the absolute frequency of reaching this state from state s with action a. The set of transitions is then updated after each step with the state transition experienced in the simulation. In doing so, a new transition $t_{s,a} = (s', 1)$ is added to the set $T_{s,a}$ the first time the agent experiences this transition. However, if this transition is already included in the set $T_{s,a}$, the absolute frequencies n are counted up. Under the condition that the environment does not change, according to the law of large numbers, the relative frequency approaches more and more the real propability, the more experiences are made [5].

The relative frequencies will be calculated as follows:

$$h(s'|s, a) = \frac{n(s'|s, a)}{\sum_{(s'_i, n_i) \in T_{s,a}} n_i} \tag{19}$$

Since the transitions are experienced on the three-lane state space and only two lanes are considered in the MDP, the state space must be divided once more. Again, the middle and left lanes, and the middle and right lanes are considered separately. For the longitudinal actions a_{ac}, a_{st} and a_{br}, one transition each is updated for the state space $S^{\text{ego}}_{\text{MDP}} \times S^{\text{adj,r}}_{\text{MDP}} \in S_{\text{MDP,r}}$ and $S^{\text{ego}}_{\text{MDP}} \times S^{\text{adj,l}}_{\text{MDP}} \in S_{\text{MDP,l}}$. For a lane change to the right $a_{\text{lc,r}}$ and a lane change to the left $a_{\text{lc,l}}$, only the transitions for the respective MDP MDP,r, and MDP,l are updated. We distinguish here between the MDP,r and MDP,l, since they can differ in principle in the choice of reward function. For example, an obligation to drive on the right lane can be represented by rewarding a lane change to the right in MDP,r, but penalizing a lane change to the left in MDP,l. Note, however, that we do not represent this in our model and in our case MDP,r equals MDP,l. In the following, we name the states s_l, s_r and the actions a_l, a_r associated with MDP,l and MDP,r. The algorithm is shown in Algorithm 1.

Algorithm 1 Model Learning Algorithm

```
Require: episodes
for each episode in episodes do
    for each step of episode do
        $a_{\text{eMDP}} \leftarrow \epsilon$- GREEDY($\tilde{Q}_{\text{C}}, \epsilon$)
        $s'_{\text{eMDP}} \leftarrow$ ENVIRONMENT($s_{\text{eMDP}}, a_{\text{eMDP}}$)
        $s'_{\text{l}}, s'_{\text{r}} \leftarrow$ DECOMPOSE($s'_{\text{eMDP}}$)
        if $a_{\text{eMDP}}$ is not a lane change then
            $a_{\text{MDP}} \leftarrow a_{\text{eMDP}}$
            UPDATE($s_{\text{l}}, a_{\text{MDP}}, s'_{\text{l}}$)
            UPDATE($s_{\text{r}}, a_{\text{MDP}}, s'_{\text{r}}$)
        else if $a_{\text{eMDP}}$ is a lane change left then
            UPDATE($s_{\text{l}}, a_{\text{lc,l}}, s'_{\text{l}}$)
        else if $a_{\text{eMDP}}$ is a lane change right then
            UPDATE($s_{\text{r}}, a_{\text{lc,r}}, s'_{\text{r}}$)
        end if
        $s'_{\text{l}} \leftarrow s_{\text{l}}$
        $s'_{\text{r}} \leftarrow s_{\text{r}}$
        if step modulo $C_{\text{steps}} = 0$ then
            changed_a_l ← VALUE_ITERATION(MDP,l)
            changed_a_r ← VALUE_ITERATION(MDP,r)
            if changed_a_l + changed_a_r == 0 then
                END_PROGRAM
            end if
        end if
    end for
end for
```

The function ϵ-GREEDY($\tilde{Q}_{\text{C}}, \epsilon$) is an exploration strategie, which selects a random action with probability ϵ and selects the action a_{eMDP} corresponding to $\tilde{Q}_{\text{C}}$ with probability $1 - \epsilon$. The function ENVIRONMENT($s_{\text{eMDP}}, a_{\text{eMDP}}$) corresponds to the simulation environment, which simulates a step from the state s_{eMDP} and the input of the action a_{eMDP} and returns the subsequent state s'_{eMDP}. A state s_{eMDP} of the extended state space is decomposed into a state $s_{\text{MDP,l}}$ for the left MDP and a state $s_{\text{MDP,r}}$ for the right MDP using the function DECOMPOSE(s_{eMDP}). The function UPDATE($s_{\text{MDP}}, a_{\text{MDP}}, s'$) updates the transition model of the model as described in Sect. 4. Finally, after a constant number of steps C_{steps}, the driving policy is recomputed using the function VALUE_ITERATION(MDP) for the updated MDP. The value iteration is an optimization algorithm for MDPs that iterates over the entire state space and updates the Q-values based on the Bellman equation until they converge. For more information on this, we refer interested readers to Sutton and Barto [18]. The function returns the number of actions (changed_a) that have changed in the policy due to the value iteration. If the number is zero for MDP,l and MDP,r the program ends.

As described earlier, the transition frequencies converge against the real transition probabilities. A simple termination condition can be the number of changed actions in the policy after the value iteration, since in that case the model has not changed fundamentally since C_{steps}.

5 Experimental Setup

In this work, we use the simulation environment Simulation of Urban Mobility (SUMO)[12]. We train the agent on episodes of a $1.1\,km$ long three-lane straight road with a total of 30 other vehicles. The ego vehicle starts at a standstill in a random lane at the beginning of the road, while the other vehicles are initialized in random lanes at random positions. The other vehicles are divided into three groups with different target speeds. The target speeds of these groups are 0.4, 0.6 or 0.8 times the maximum ego speed $v_{\text{max}} = 50\,\frac{\text{km}}{\text{h}}$. The other cars cannot change their lane, but can accelerate and decelerate with the internal motion planner. All cars have the same vehicle length $l_{\text{car}} = 5\,m$. The lane change time for the ego vehicle is $3\,s$, all other actions are simulated with a time of $1\,s$.

We model the MDP with a discount factor of $\gamma = 0.9$. As an exploration strategie, we use epsilon-greedy, which was described in 4. The ϵ decreases linearly over 2,000,000 steps, where it is initially $\epsilon_{\text{start}} = 0.9$ and at the end $\epsilon_{\text{end}} = 0.1$. Upwards of $2,000,000$ steps the epsilon remains constant at ϵ_{end}.

Each learning episode is randomly initialized with a different random seed, so they are always different. Every 500,000 steps the driving strategy is relearned by value iteration, and the MDP is stored. Every stored MDP is then evaluated using 1000 episodes with the greedy strategy, where each of these episodes has a different random seed that is not included in the random seeds of the learning episodes. However, to make the evaluations comparable, each evaluation is initialized with the same random seeds.

6 Results

In this section, we show the results obtained based on the experimental setup 5. Figure 3 plots the average reward and velocity and the fraction of collision-free episodes to each evaluation. It shows that the reward increases strongly in the first 4,000,000 steps. The fraction of collision-free episodes increases to about 98 % in the same period, which explains the increase in the average reward due to the strong penalty of a collision. At the same time, the average speed decreases during this period and reduces the reward negligibly due to a lower R_{v}. The policy has become more defensive due to negative experiences in collision states, so speed was reduced earlier in critical situations to avoid collisions.

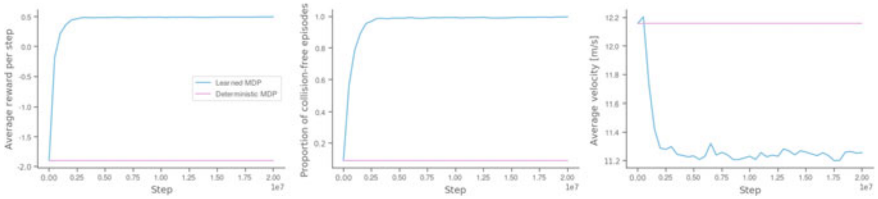


Fig. 3 Average reward, collision-free episodes, and average velocity

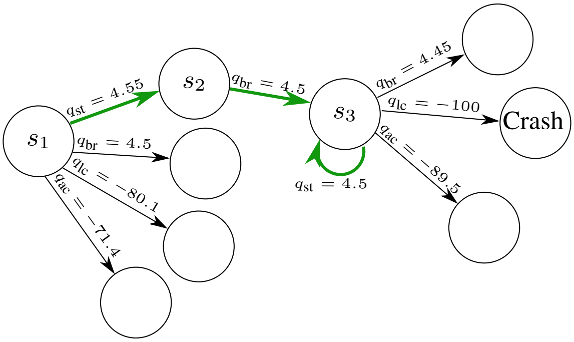


Fig. 4 Three states of the deterministic MDP

After $4,000,000$ learning steps, the average speed does not decrease further but remains approximately constant. However, as the proportion of collision-free episodes tends to increase, the average reward per step also increases. The training is completed after 20,000,000 steps with a proportion of 99.8 % collision-free episodes.

The learned model can now be examined in every state. Here, we exemplify how the driving strategy could be improved by means of a simple example. Figure 4 shows a small section of the deterministic MDP in the states s_1, s_2, and s_3. Here, only selected transitions and subsequent states are shown for clarity. In Table 1, we show the corresponding states. Vehicle 3 has the minimum speed and maximum distance to the ego vehicle in these states. Since it thus has no influence on the decision, it is not considered here.

In the deterministic MDP, there are four subsequent states corresponding to the four possible actions in each state. In the graph, the action values q_{ac}, q_{st}, q_{br}, q_{lc} are noted at the edges of the transitions, which were calculated for each action by value iteration. The green transitions represent the actions with the maximum action value that, according to the model, maximize the reward over time and that the agent would choose according to the greedy algorithm. In state s_1, the ego vehicle has a distance of $\tilde{d} = 35\,m$ to the front vehicles, vehicle 1 and vehicle 2, and the relative speed is $\tilde{v} = -25\ \frac{\text{km}}{\text{h}}$. So the ego vehicle is driving toward the front vehicle. Since the vehicles are at the same height and cannot be overtaken, an acceleration process is evaluated badly, since the ego vehicle would have to brake from a higher speed after this process. Similarly, a lane change is evaluated poorly because it takes a relatively long time in

Table 1 Decomposed states s_1, s_2 and s_3

	$\tilde{v}_{\text{ego}}[\frac{\text{km}}{\text{h}}]$	$\tilde{d}_1[\text{m}]$	$\tilde{v}_1[\frac{\text{km}}{\text{h}}]$	$\tilde{d}_2[\text{m}]$	$\tilde{v}_2[\frac{\text{km}}{\text{h}}]$
s_0	40	45	−25	45	−25
s_1	40	35	−25	35	−25
s_2	40	25	−25	25	−25
s_3	35	15	−15	15	−15

which the agent cannot slow down. The best decision according to the deterministic MDP is to maintain speed. After this decision, the agent predicts that it will enter state s_2, where the relative velocity remains the same and the distance decreases to $\tilde{d} = 25\,\text{m}$. In this state, only deceleration is still evaluated well, leading the agent in the MDP to state s_3, where the distance to both front vehicles is only $\tilde{d} = 15\,\text{m}$, but the relative velocity is also only $\tilde{v} = -15\,\frac{\text{km}}{\text{h}}$. Due to the coarse quantization, the velocity difference is not sufficient to move to a smaller distance state when holding the velocity in the MDP. If this strategy is used in the simulation, it will inevitably lead to a collision.

Figure 5 shows the learned model after 500,000 steps in the same states. In addition to the action values, the transition probabilities to a transition are also shown in this graphic. An action can now have several transitions to different subsequent states as indicated by the short arrows. It can be seen that in the same state s_1 it is no longer the best action to maintain the velocity but to decelerate. The reason becomes evident by observing the new transitions.

s_3 has now multiple transitions for action a_{st}, where 22 % of the transitions lead to s_3 as in the deterministic MDP, but 33 % of them lead to a crash. The other transitions, which are only hinted in the figure, lead to other states that are rated poorly as well. With a weighting of the rewards with the probabilities, s_3 is now no longer a favorable state, which also decreases the action values leading to s_3. The best action for state s_3 is a_{br} with an action value of $q_{\text{br}} = -20.8$, since it has no direct transitions to the crash state. However, some subsequent states still lead to collisions later on, so that the action value still remains negative.

By braking in state s_1, the agent significantly improves its situation. The magnitude of the differential velocities to vehicle 1 and 2 becomes smaller, so that a collision becomes less likely with further braking. However, the agent can still get into similar bad states as s_2 and s_3 afterward. For example, if vehicles 1 and 2 also brake. Consequently, the agent should not be in s_1 in the first place. If we look at s_0, where one subsequent state for the action a_{st} is s_1, we see that the agent would have already slowed down at a greater distance to the vehicles 1 and 2.

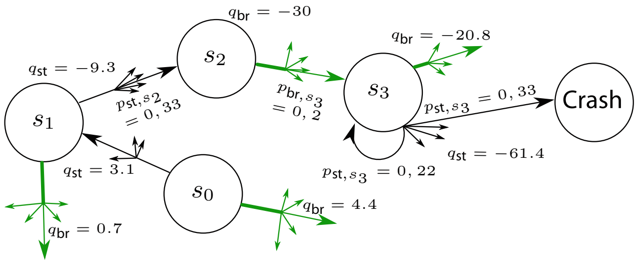


Fig. 5 Three states of the learned MDP after 500,000 learning steps

7 Discussion

Section 6 has shown that learning the transition model of the MDP can significantly improve the driving strategy. The learned MDP was able to handle 99.8% of episodes collision-free at a high average speed after simulation. Early on, in states that were considered safe in the deterministic MDP, state-action pairs were experienced that led to unsafe states, where a collision was unavoidable. As a result, the driving policy became more defensive and the agent avoided actions that could lead to collisions. In the deterministic MDP, on the other hand, due to the coarse quantizations and only one transition represented, a safe driving policy cannot be found, because safe actions in the MDP can be unsafe in the real environment. The model is completely transparent so that any decision based on the MDP can be easily understood. We could demonstrate this with a simple example of how the strategy changed due to new transitions in the MDP.

We were also able to show how a driving strategy for a three-lane road could be generated based on the modeled MDP for a two-lane road. Thus, 5 instead of only 3 additional vehicles could be considered without increasing the complexity of the model.

A major advantage to the MDP is that once experience is gained, it is not forgotten, so it becomes more accurate with each new experience and more knowledge about the environment is gained. However, experience in state space regions where little experience has been gained before is more important for learning the model than experience from state space regions that are already known. These state space regions were not explicitly searched for by the epsilon-greedy strategy, so the agent spent a lot of time in regions where the model was already sufficiently known. To address this problem, exploration strategies are needed that specifically target state space regions about which little is known.

8 Conclusion and Future Work

In this paper, we have shown how expert knowledge can be used to model an MDP for solving tactical maneuver planning on a two-lane road. To do this, we were able to not only apply the MDP modeled for a two-lane road to three-lane roads for decision making, but also learn the transition model of the MDP within a simulation environment to obtain an improved driving strategy. We have shown that the learned MDP performs significantly better than the simple deterministically modeled MDP. Due to the complete transparency of the model, we were able to examine the MDP and show by example how the newly learned transitions have a positive impact on the resulting driving strategy.

In the future work, we would like to investigate the impact of exploration strategies such as $R_{\max}$ and Bayesian reinforcement learning on the learning process of MDPs, especially to learn transitions from states where little is known about the transition model. We also aim to represent tactical maneuver planning as a factorized Markov decision process to reduce the complexity of the model and speed up the learning process.

References

1. Araya-López M, Buffet O, Thomas V, Charpillet F (2012) Active learning of MDP models. In: Sanner S, Hutter M (eds) Recent advances in reinforcement learning. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 42–53
2. Brechtel S, Gindele T, Dillmann R (2011) Probabilistic MDP-behavior planning for cars. In: 2011 14th international IEEE conference on intelligent transportation systems (ITSC), pp 1537–1542 (2011). https://doi.org/10.1109/ITSC.2011.6082928
3. Buehler M, Iagnemma K, Singh S (2009) The DARPA urban challenge: autonomous vehicles in city traffic, George Air Force Base, Victorville, California, USA, vol 56. Springer, Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03991-1
4. Claussmann L, Revilloud M, Gruyer D, Glaser S (2020) A review of motion planning for highway autonomous driving. IEEE Trans Intell Transp Syst 21(5):1826–1848. https://doi.org/10.1109/TITS.2019.2913998
5. Dekking FM, Kraaikamp C, Lopuhaä HP, Meester LE (2005) A modern introduction to probability and statistics—understanding why and how. Springer Science & Business Media, Berlin, Heidelberg
6. Guan Y, Li S, Duan J, Wang W, Cheng B (2018) Markov probabilistic decision making of self-driving cars in highway with random traffic flow: a simulation study. J Intell Connected Veh 1:77–84. https://doi.org/10.1108/JICV-01-2018-0003
7. Hoel CJ, Driggs-Campbell K, Wolff K, Laine L, Kochenderfer MJ (2020) Combining planning and deep reinforcement learning in tactical decision making for autonomous driving. IEEE Trans Intell Veh 5(2):294–305. https://doi.org/10.1109/TIV.2019.2955905
8. Hoel CJ, Wolff K, Laine L (2018) Automated speed and lane change decision making using deep reinforcement learning. In: The thirty-first IEEE international conference on intelligent transportation systems. Maui, Hawaii, United States, pp 2148–2155. https://doi.org/10.1109/ITSC.2018.8569568
9. Hubmann C, Becker M, Althoff D, Lenz D, Stiller C (2017) Decision making for autonomous driving considering interaction and uncertain prediction of surrounding vehicles. In: 2017 IEEE

intelligent vehicles symposium (IV), pp 1671–1678 (2017). https://doi.org/10.1109/IVS.2017.7995949

10. Krasowski H, Wang X, Althoff M (2020) Safe reinforcement learning for autonomous lane changing using set-based prediction. In: 2020 IEEE 23rd international conference on intelligent transportation systems (ITSC), pp 1–7 (2020). https://doi.org/10.1109/ITSC45102.2020.9294259
11. Liu W, Kim SW, Pendleton S, Ang MH (2015) Situation-aware decision making for autonomous driving on urban road using online POMDP. In: 2015 IEEE intelligent vehicles symposium (IV), pp 1126–1133 (2015). https://doi.org/10.1109/IVS.2015.7225835
12. Lopez PA, Behrisch M, Bieker-Walz L, Erdmann J, Flötteröd YP, Hilbrich R, Lücken L, Rummel J, Wagner P, Wießner E (2018) Microscopic traffic simulation using sumo. In: The 21st IEEE international conference on intelligent transportation systems, pp 2575–2582. IEEE (2018). https://doi.org/10.1109/ITSC.2018.8569938. https://elib.dlr.de/124092/
13. Moerland TM, Broekens J, Jonker CM (2020) Model-based reinforcement learning: a survey (2020). arXiv abs/2006.16712. https://arxiv.org/abs/2006.16712
14. Paden B, čáp M, Yong SZ, Yershov D, Frazzoli E (2016) A survey of motion planning and control techniques for self-driving urban vehicles. IEEE Trans Intell Veh 1(1):33–55 (2016). https://doi.org/10.1109/TIV.2016.2578706
15. Schwarting W, Alonso-Mora J, Rus D (2018) Planning and decision-making for autonomous vehicles. Ann Rev Control Rob Auton Syst 1(1):187–210. https://doi.org/10.1146/annurev-control-060117-105157
16. Statistisches Bundesamt (2021) Verkehrsunfälle–Fachserie 8 Reihe 7–2020 p 49. https://www.statistischebibliothek.de/mir/servlets/MCRFileNodeServlet/DEHeft_derivate_00063182/2080700207004_akt01112021.pdf
17. Sutton RS (1991) Dyna, an integrated architecture for learning, planning, and reacting. ACM SIGART Bull 2(4):160–163. https://doi.org/10.1145/122344.122377
18. Sutton RS, Barto AG (2018) Reinforcement learning: an introduction. A Bradford Book, Cambridge
19. Ulbrich S, Maurer M (2015) Towards tactical lane change behavior planning for automated vehicles. In: 2015 IEEE 18th international conference on intelligent transportation systems, pp 989–995. https://doi.org/10.1109/ITSC.2015.165

Fake Review Detection with Concept Drift in the Data: A Survey

Ketan Sanjay Desale, Swati Shinde, Nikita Magar, Snehal Kullolli, and Anjali Kurhade

Abstract Online reviews have a great impact on the e-commerce industry. Online users are free to post their perspective on products, which might not always be unbiased or accurate. Such unbiased reviews from the customers can affect both buyers and sellers in the industry. The details of this paper focus on a fake review detection system. This paper examines different techniques used in fake review detection which involves data pre-processing to pre-process and extract features from raw data, classification to classify review as fake or real. Also, our study deals with drift in data, its detection methods, as well as drift adaptation strategies.

Keywords Data pre-processing · Classification · Concept drift detection · Concept adaptation

1 Introduction

A customer's choice of a product is heavily influenced by product reviews online. However, since people are free to express their opinions about the product , the reviews might not always be accurate or unbiased. This can have negative consequences for both customers and services, posing a challenge in the e-commerce industry. It is crucial to take customer reviews into account seriously. However, online reviews can also be abused by adversaries for various reasons. Therefore, it is essential to distinguish between genuine and dubious reviews.

Our survey paper presents a survey of data processing techniques and classification techniques associated with fake review detection. The goal is to analyse and explore data pre-processing, classification methods, as well as concept drift detection and adaptation techniques that will help the model to improve its performance.

The use of machine learning algorithms has been extensively studied for the detection of deceptive and/or fake reviews [1]. Deep learning algorithms have also

K. S. Desale (✉) · S. Shinde · N. Magar · S. Kullolli · A. Kurhade
Pimpri Chinchwad College of Engineering, Pune, India
e-mail: ketan.desale@pccoepune.org

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_63

been proven useful for detecting deceptive reviews. These learning algorithms take review data as input and classify the data into fake or real reviews. However, data can change over time. It does not last forever. No matter how carefully constructed, the model is on mounds of well-labelled data. With time, its predictive power declines. A model can decay in one of two ways. One is due to data drift, and the other is due to concept drift. Data drift occurs when data evolves overtime, potentially introducing previously unseen types of data and new categories. It will not affect previously labelled data, however. Concept drift occurs when our interpretation of data changes over time while the distribution of data remains the same. As a result, the user-end interprets that model predictions have become worse over time for similar data. To resolve this problem, old data must be re-labelled and the model retrained.

This paper is divided into the following sections: Related work section gives a brief technical background of fake review detection systems which includes data pre-processing, machine learning, deep learning and concept drift detection. Finally, the conclusion section sheds some light on future work.

2 Related Work

Here, we are discussing about the techniques used in modelling a fake review detection system. We are starting by discussing data pre-processing, classification techniques, and finally, concept drift detection and adaptation.

2.1 Data Pre-processing

Data pre-processing is a technique for converting raw data into a format that will improve the model's accuracy. Data pre-processing is the first and crucial step while working with a machine learning model. It is the process of preparing a row data set and making it suitable for analysis. Tokenization [2] is the basic and first step before applying any other pre-processing technique. The sentences are divided into words and paragraphs are divided into sentences and converted words and sentences are called "Tokens". Sometimes data is very unbalanced for the classification. So to resolve this problem, in [3], they have applied two methods were over-sampling and under-sampling. Stemming is the process that reduces or convert the world in the original form [4]. Example : "Chocolatey"; "Choco" converted into "Choco-late".

Feature Extraction Feature extraction reduces the number of features in a data set by constructing new features based on existing features. Most of the existing features have lower accuracy due to that they just use a single feature [5]. TF-IDF stands for term frequency-inverse document frequency. It takes a text as input and converts it into a matrix by calculating the logarithmic value or table no of words and re-reviews. If the word is very common or it is repeating many times, then its value will be 0; otherwise, it will be 1 [6].

Table 1 Comparison of data pre-processing techniques

Ref.	Year	Algorithm	Pre-processing	Data set	Metric	Result (%)
Ligthart et al. [5]	2021	NB NB + Self training	Tokenization, lemmatization, stop word removal	Yelp gold standard	Accuracy	73.00 93.00
Elmogy et al. [2]	2021	LR NB KNN(K=7) SVM RF	Tokenization, Lemmatization, stop word removal	Yelp	F1-score	82.00 80.38 81.26 80.82 80.79
Wang et al. [7]	2020	Supervised Semi-supervised	Sentiment analysis	Yelp Res	Accuracy	61.00 71.41
Wang et al. [7]	2020	Supervised Semi-supervised	Sentiment analysis	Yelp Chi	Accuracy	81.07 82.53
Le et al. [8]	2020	SVM ANN RF DT	Clustering	Yelp	Accuracy	87.30 88.70 92.55 88.30
Viji et al. [6]	2020	LR NB DT XG Boost Ada Boost SVM	Sentiment analysis	Amazon	Accuracy	84.30 83.20 77.60 84.53 84.54 84.88
Sihombing et al. [3]	2019	SVM LR XG Boost NB	Over-sampling, under-sampling	Yelp	F1-score	77.00 78.00 99.00 65.00

NB Naive Bayes, *LR* Logistic regression, *KNN* K-nearest neighbours, *SVM* Support vector machine, *RF* Random forest, *ANN* Artificial neural network, *DT* decision tree

Table 1 contains some techniques and their accuracy, which are based on the data reviewed by us. Here, they demonstrate the accuracy of the classifiers using the full clustering capability, which improves performance [8]. They found that random forest classification provided the highest accuracy. The naive Bayes classifier gives a 93% accuracy on the gold standard data set, whereas it gives 73% accuracy on Yelp [5]. When authors have applied the supervised and semi-supervised classification algorithms on the Yelp Chi data set, they achieved 81.07% and 82.53% accuracy, respectively, while when applied it to Yelp Res, they achieved 61% and 71.41% accuracy, respectively. The accuracy of the model was obtained with the presence of extracted features, which used the Bi-gram language [2]. Here, LR with extracted features gave the best accuracy on the Yelp data set. XGBoost classifier gave the 99% F1-score on the Yelp data set while others gave 78% on average [3].

2.2 Classification

Classification is applied to both unstructured and structured data. Classification is the process of classifying data into a set of different categories. A classification problem involves determining which category or class a piece of data belongs to. A classifier maps input data to a specific category. The classification model tries to make a prediction based on the input values. It will predict the class labels categories for the new data. Following are some techniques for improving the performance of classifiers:

Using certain hyper parameter In machine learning, a hyperparameter determines the value of model parameters and the algorithm learns these parameters. The number of estimators can be increased in random forest to increase accuracy. Accuracy is independent of the maximum depth of the tree in RF. A high maximum depth of the tree with few estimators or a low depth with a great number of estimators can give high performance in XGBT. In the decision tree, maximum depth does not affect the performance much [1].

Use of boosting techniques Boosting consists of combining several weak learners into a single strong learner to minimize training errors. It involves selecting a random sample of data, fitting it with a model, and training it sequentially so that each model tries to make up for the shortcomings of the previous one. The AdaBoost algorithm fits the estimators sequentially using the whole data set, so the ensemble can fit it to the best of its ability. AdaBoost performs well when ensemble with SVM or MLP than bagging. Because MLP AdaBoost ensemble is well suited for training data with 14 or more estimators [1]. Bagging refers to the process of choosing a random sample of data from a training set with replacement, that is each data point can be chosen more than once.

Semi-supervised methods Semi-supervised learning is a machine learning algorithm. The model learning algorithm must predict the future from a small number of labelled instances and a large number of unlabelled examples in a semi-supervised learning issue. In semi-supervised learning, self-training is a classical approach with many applications. A self-training algorithm generates pseudo-labels for the unlabelled examples and gradually refines them so they coincide with the actual labels. The only semi-supervised method that outperforms the traditional supervised classification methods is self-training [5].

Unsupervised Methods Unsupervised learning, also called unsupervised machine learning, focuses on analysing and clustering unlabelled data sets using machine learning algorithms. Using these algorithms, data patterns or groups of data can be discovered without the involvement of a human. With its ability to discern similarities and differences in information, it is the perfect tool to conduct exploratory data analysis, cross-selling strategies, and customer segmentation. First, a simple classifier is trained to distinguish between old and new data sets. A drift is detected concerning classifier performance [9].

Table 2 Comparison of accuracy of different data sets

Model	Data sets	Accuracy
CIDD-ADO-DNN [10]	Spam data set	0.9320
	Chess data set	0.7646
	KDDCup99 data set	0.9592

Deep learning method Deep neural network (DNN) in deep learning can be used in classification for fake review detection. Optimal parameters help in increasing performance of the DNN model. ADO-DNN can determine the actual class labels and ADO helps to gain improved classifier performance [10]. Table 2 states the comparison of accuracy using ADO-DNN method on various data sets.

CNNs are a class of deep, feedforward artificial neural networks where there are no cycles between nodes. Through the use of CNN models, a novel algorithm and performance approach can be used to predict heart disease [11]. Long short-term memory is a type of recurrent neural network that is better at memory than traditional recurrent neural networks. Having a good grasp of patterns, LSTMs can perform fairly well. A multi-layer perceptron classifier is a neural network that is built into the algorithm. MLP classifier, unlike other methods like support vectors or naive Bayes classifier, requires an underlying Neural network to execute the classification task. CNN, LSTM and MLP methods are applied on the Yelp data set using some techniques under certain conditions. It is observed that LSTM performs well on the Yelp data set when the train test ratio is 80:20 using the word2vec technique [12].

2.2.1 Use of Clustering Techniques

Clustering or cluster analysis is a machine learning technique for grouping unlabelled data. Data clustering is the process of arranging data points into groups consisting of similar data points. SVM functions as both a linear and a non-linear classification method in machine learning. SVM algorithm finds hyper-planes that separate multi-dimensional data into classes. SVM is a commonly used classification algorithm for fake review detection [8]. Random forest outperformed SVM and neural network in terms of accuracy and recall, with 92.55% and 95.27%, respectively. When the cluster labels are removed from the separate feature sets, the accuracy and other measures decline marginally [8].

2.3 Concept Drift Detection

Concept drift is a concept used during predictive analytics & machine learning to characterize how the statistical properties of the target variable that the machine learning is trying to protect change over time in unforeseen ways (Fig. 1).

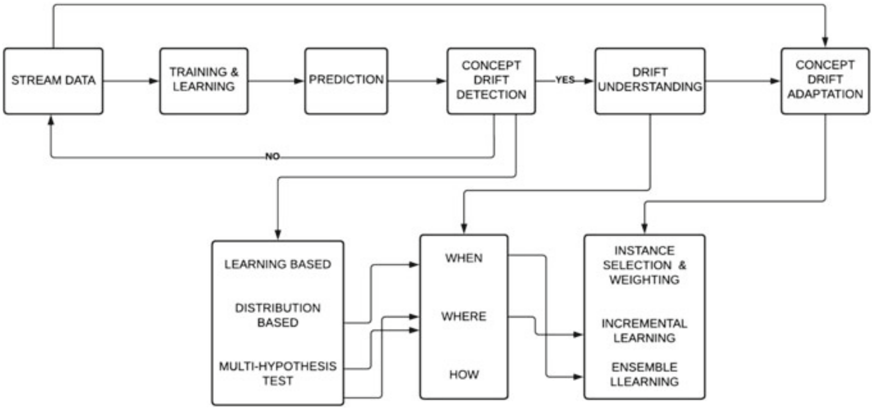


Fig. 1 Framework of concept drift detection

Types of Drifts:

1. Incremental Drift: It implies a long drift duration, the change is gradual and continuous. It is also known as continuous drift.
2. Sudden Drift : A drift is sudden, with no time overlap between two different distributions.
3. Gradual Drift : A change that happens progressively from one process to another over a period of time.
4. Recurring Drift : Defines if both contexts are from the same distribution to use a multivariate non-parametric test.

Methods of Concept Drift Detection:

1. Sequential Analysis Method:
   - This detector analyses to see whether model's error rate is stable and alerts us if it is not.
   - This category comprises DDM (Drift detector method), EDDM (Early drift detector method), CUSUM (Cumulative sum) and PHT (Page Hinkley) methods.
2. Method to Statistical Analysis:
   - To detect concept drift, this approach examines the standard deviation and mean the predicted results.
   - This category includes the methods like DDM (Drift detector method), EDDM (Early drift detector method), PH (Page Hinkley), STEPD, MDDM (McDiarmid's Drift detector method), RDDM (Reactive Drift detector method) and EWMA (Exponentially weighted moving average).

3. Window-Based Method Analysis:
   - A window method is used to preserve recent data for retraining and old data for distribution change.
   - Adaptive windowing, FHDDM (Fast hoeffding's drift detection method), SEED, HDDM.

Following can be the steps to detect fake review:

1. Study how a characteristic changes over time in data.
2. Examine the problem of concept drift in the detection for fake review.
3. Investigate the relationship between concept drift and review classification performance.

In [13], authors analysed the predictive accuracy, number of drifts, evolution time and memory use of various drift detection methods.

3 Conclusion

The main aim of this paper was to explore recent technologies which are involved in building the model for detecting reviews as fake or real. But as time changes, review data also changes. This leads to a decline predictive power of the model. Concept drift occurs when our interpretation of data changes over time while the distribution of data remains the same. So, to detect concept drift and to adapt the drift different methods are also explored in this paper. Based on studied papers, we conclude that deep learning performs better than machine learning algorithms in classifying reviews and for data pre-processing tokenization, stopword removal, lemmatization and TF-IDF techniques gave the best results. Among different drift detection methods, DMDDM method gave the best result. In future, we are going to propose a model that will work on the Yelp data set. Our model will consist of data pre-processing techniques; they are tokenization, stop word removal, lemmatization, TF-IDF. Then using LSTM, classifier data will be classified. If concept drift is present, then it will be detected by DMDDM, and using adaptation technique, it will be adapt, and our model will get an update.

References

1. Gutierrez-Espinoza L, Abri F, Siami Namin A, Jones KS, Sears DRW (2020) Ensemble learning for detecting fake reviews. In: 2020 IEEE 44th annual computers, software, and applications conference (COMPSAC), pp 1320–1325. https://doi.org/10.1109/COMPSAC48688.2020.00-73
2. Elmogy A, Tariq U, Mohammed A, Ibrahim A (2021) Fake reviews detection using supervised machine learning. Int J Adv Comput Sci Appl 12(1):601–606

3. Sihombing A, Fong ACM (2019) Fake review detection on yelp dataset using classification techniques in machine learning. In: 2019 international conference on contemporary computing and informatics (IC3I), pp 64–68. https://doi.org/10.1109/IC3I46837.2019.9055644
4. Navale G, Kurkute S, Amey R, Kamble K (2020) Detection of fake reviews using machine learning algorithm. Int J Future Gener Commun Netw 13(1):415–419
5. Ligthart A, Catal C, Tekinerdogan B (2021) Analyzing the effectiveness of semi-supervised learning approaches for opinion spam classification. Appl Soft Comput 101. https://doi.org/10.1016/j.asoc.2020.107023. https://www.sciencedirect.com/science/article/pii/S1568494620309625
6. Viji D, Asawa N, Burreja T (2020) Fake reviews of customer detection using machine learning models. Int J Adv Sci Technol 29(6):86–94. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/11297
7. Wang J, Kan H, Meng F, Mu Q, Shi G, Xiao X (2020) Fake review detection based on multiple feature fusion and rolling collaborative training. IEEE Access 8:182625–182639. https://doi.org/10.1109/access.2020.3028588
8. Le H, Kim B (2020) Detection of fake reviews on social media using machine learning algorithms. Issues Inf Syst 21(1):185–194. https://doi.org/10.48009/1is202185-194
9. Gözüaçk Ö, Büyükçakır A, Bonab H, Can F (2019) Unsupervised concept drift detection with a discriminative classifier. In: Proceedings of the 28th ACM international conference on information and knowledge management (CIKM '19). Association for computing machinery, New York, NY, USA, 2365-2368. https://doi.org/10.1145/3357384.3358144
10. Priya S, Uthra RA (2021) Deep learning framework for handling concept drift and class imbalanced complex decision-making on streaming data. Complex Intell Syst. https://doi.org/10.1007/s40747-021-00456-0
11. Desale KS, Shinde SV (2022) Addressing concept drifts using deep learning for heart disease prediction: a review. In: Gupta D, Khanna A, Kansal V, Fortino G, Hassanien AE (eds) Proceedings of second doctoral symposium on computational intelligence. Advances in intelligent systems and computing, vol 1374. Springer, Singapore. https://doi.org/10.1007/978-981-16-3346-113
12. Shahariar GM, Biswas S, Omar F, Shah FM, Binte Hassan S (2019) Spam review detection using deep learning. In: 2019 IEEE 10th annual information technology, electronics and mobile communication conference (IEMCON), pp 0027–0033. https://doi.org/10.1109/IEMCON.2019.8936148
13. Mohawesh R, Tran S, Ollington R, Xu S (2021) Analysis of concept drift in fake reviews detection. Expert Syst Appl 169. https://doi.org/10.1016/j.eswa.2020.114318. https://www.sciencedirect.com/science/article/pii/S0957417420310137

A Survey on Research Directions in Blockchain Applications Usability

Vivek Sharma and Tzipora Halevi

Abstract This research systematically reviews blockchain usability studies published between 2017 and 2021. It analyzes direction trends aimed at improving the overall blockchain application's real-world adoption. After determining the inclusion and exclusion criteria, 22 articles were included in the review. This work presents the major existing challenges found in Blockchain applications, such as privacy issues and non-regulation, and the proposed solutions, including increased transparency and simple usable applications. Major findings include the fact that user surveys are the most popular method among these studies compared to expert surveys or observational studies. Most of the current blockchain usability studies are performed for applications related to the financial domain, followed by health care, supply chain applications, energy, and e-voting. The majority of these studies include less than 20 participants for the expert-based and less than 40 for user-based ones. This study further investigates the domain-specific target systems. The healthcare-related surveys concentrated on the usability of users' data on electronic medical record (EMR). In the financial field, the focus was mostly on the use of crypto wallets or crypto applications. The main concern among participants in healthcare-related applications was the privacy of their medical data while in finance, the concern was the lack of a local regulatory body. This research has important implications that can help researchers address challenges and implement appropriate solutions, which can improve their adoption rate.

Keywords Blockchain · Usability · User perception · Blockchain-based application

V. Sharma
Department of Computer Science, The Graduate Center, City University of New York, NY, USA
e-mail: vsharma@gradcenter.cuny.edu

T. Halevi (✉)
Department of Computer Science, Brooklyn College, City University of New York, NY, USA
e-mail: halevi@sci.brooklyn.cuny.edu

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_64

1 Introduction

Blockchain technology is one of the most talked-about technologies in recent times. While its most commercially successful implementation is in finance, the technology has been gaining popularity in applications in other domains. However, the adoption of blockchain is still in its nascent stage. A recent report [1] shows 11.2% of Americans own at least one cryptocurrency. Similar estimates are provided for UK and France (less than 10%) and Germany (less than 5%).

Many blockchain-based applications were introduced in recent years in a diverse range of domains such as security, finance, e-voting, IoT, energy, health, supply chain management, manufacturing, and digital copyright. But even with multiple use cases and a promising advantage of bringing security, integrity, and de-centralization, this technology still fails to replace the current legacy systems employed. The adoption rate, despite growing tremendously in some areas like finance, remains limited in other areas. Usability studies are considered an important step before wide deployment of applications. Therefore, this study examines and summarizes the current usability studies and their implications regarding issues that impede wide real-world adoption of these blockchain applications

Usability testing is a methodology that helps improve applications design and produces intuitive and user-friendly products. Usability studies are often fundamental to the product success, and therefore incorporating them into the development process can be very beneficial. A standard usability test may incorporate five steps, including recruiting participants, designing testing procedures, conducting the test session, analyzing the results, and presenting the conclusions and recommendations.

This paper aims to study the current state of the research including challenges and proposed solutions in the usability of blockchain-based applications by summarizing published articles in various journals.

Research Questions: This paper looks at the following research questions:

1. What is the current research state for the usability of blockchain applications?
2. What are the challenges and problems related to these applications?
3. What are the proposed solutions that have been published?
4. What are the future research direction in this area?

2 Theoretical Background

Blockchain, in its plain form, is an immutable, publicly available distributed ledger. The first major application conceptualized was bitcoin [2], which turned out to be the most famous application of blockchain till now. According to an article in the Finance Online [3], there are 68 million Bitcoin wallet users as of February 2021. While this number may not seem significantly large, it is a great increase from the 26 million that was recorded in July 2018. As other cryptocurrencies gained popularity through the years, it is estimated that there are a total of 200 million crypto users today [4].

2.1 Usability Testing Methods

Usability testing includes both quantitative and qualitative forms [5]. Qualitative methods are used to gain insights, analyze the quality of the system, and discover usage problems. Quantitative analysis collects metrics that aim to quantify the user experience of the system. [6] lists some common usability metric. The most basic metrics are:

- Success Rate
- Time a task requires
- Error Rate
- User's subjective satisfaction

For quantitative testing, Nielsen recommends having at least twenty participants [6] Another dimension of categorization is remote and in-person testing. While in-person testing is expensive due to needing a moderator as well as a physical environment like a laboratory to conduct a well-planned test, remote testing is further divided into moderated or unmoderated. Moderated testing is similar to in-person testing, but the testing environment is native to the user's environment. Remote unmoderated testing employs a tool that a participant can use at their convenient time. This tool is responsible for collecting the specific data from the participants in a predetermined format, which eliminates the need for a moderator.

Nielsen proposed seven inspection methods [5] as part of usability testing methods. These methods were heuristic evaluation, cognitive walkthrough, formal usability inspections, pluralistic walk-through, feature inspection, consistency inspection, and standard inspection.

SUS study, created by John Brooke, works with small sample size and is easier to scale [7]. However, the scoring method is complicated, mostly in terms of interpreting. The method provides a combined usability score which is compared against a threshold to rate the usability of the system.

3 Methodology

The research adopts the methodology specified by B.Kitchenham [8] to perform a systematic review on the subject. The following subsection discusses the search strategy employed to find relevant papers in the field.

3.1 Search Strategy

- Keyword Search: The following search strings were used to find relevant papers: ”Blockchain Usability” OR ”Blockchain Application”
- Period: Papers published between 2017 and 2021 are selected
- Paper Type: Articles published in conferences or journals
- Search Database: ACM Digital Library, Google Scholar, IEEExplore, ScienceDirect, Scopus, SpringerLink
- Inclusion Criteria:
  - Articles that were published between 2017–2021 in English.
  - Article scheduled to be published.
  - Papers that include keywords in full-text and their metadata.
  - Blockchain papers talk about the usability of any blockchain technology in different domains, including ones that propose new applications, address adoption issues or give insight into any challenges from the user’s perspective.
- Exclusion Criteria:
  - Systematic Reviews were excluded from the study.
  - Papers that do not perform any usability analysis.

Using the keyword search strategy, we found 140 papers across all the databases which were related to this keyword. We manually went through each of them to read their abstract and filtered and selected 22 studies that were based on the usability of blockchain-based applications.

4 Results

Twenty-two papers were selected from various fields like health care, supply chain, finance, user perception on blockchain adoptability, identity management, e-voting, energy, tourism, and programming.

4.1 Current Research Direction

Research in different contexts When examining studies related to specific fields, we find that most studies were related to finance, followed by health care and supply chain. This result is evident in Fig. 1. A few studies examined different aspects related to user perception and proposed design guidelines for general blockchain applications. These findings point to increased exploration of blockchain-based solutions for the health care and supply chain industry. The multi-context category includes

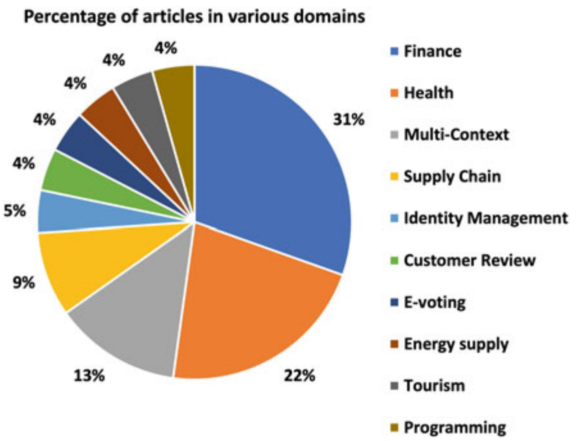


Fig. 1 Percentage of studies in each of the domains

studies that look at general blockchain application design and is applicable to more than one context.

Usability Testing Methods There were four main types of methods that were observed in the research. The distribution of the research methods types tested in the studies is shown in Fig. 2.

- **Novice user-based survey**: These include studies where the participants are users with limited or no experience working with blockchain-based applications. This category also includes casual crypto users.
- **Expert-based survey**: Experts are participants with rich knowledge in the field of blockchain. They are professionals working in the industry or researchers with expertise in the field.
- **Observational Study**: Study with non-expert users. In this case, the users are instructed to perform some set of actions and their behavior is observed for each task.
- **Analytical**: Articles categorized under this section are mainly theoretical studies based on previous research or cognitive walk-through by the authors of the article.

Figure 2 shows that the user-survey is the most common method. We also note that every observational study was paired with a user-based survey.

Average of Citations To assess the usability of the research by authors, we survey the number of citations. To this end, we use two properties: the total number of citations for the different domains, and the average number. To provide more reliable data, we only calculated this for the domains for which there was more than one usability paper included.

Table 1 shows average citation that articles from each domain got, indicating that finance has the highest number of average citation (9.5), with 67 total citations for the articles in this domain.

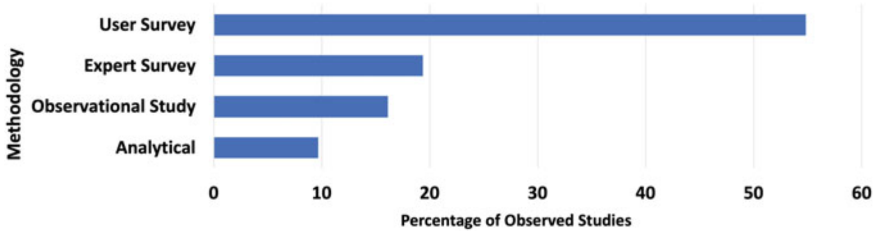
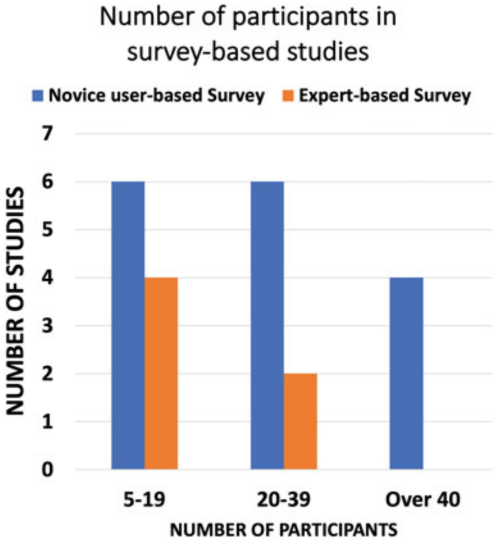


Fig. 2 Methods used in the usability studies

Table 1 Average citation to studies from various domains

Domain	Total no. of citations	Average no. of citations
Supply chain	2	1
Health care	10	2
Multi-context	13	4.33
Finance	67	9.5

Fig. 3 Count of novice user and expert participants in survey-based studies



Usability Test Participants There were two types of participants in the survey-based studies: novice user-based and expert-based surveys. Figure 3 shows the breakdown of the number of participants according to study size. Most of the expert-based surveys (4 out of 6 surveys) were found to have less than 20 participants. In contrast, the user-based studies tend to have more participants with multiple studies having over 40 participants each.

Another interesting point to note is that only 9 out of 17 user-survey studies mention a separate count for males and females. This points to a limited focus on the role of gender in application usability. While blockchain is viewed as a potential solution against gender-bias [9], women have been shown to be significantly under-represented in the crypto space [10]. Studying the effect of gender and ethnicity may help make newly developed applications more inclusive.

4.2 Usability Challenges

Researchers have been working on detecting challenges and proposing solutions aimed at increasing blockchain applications adoption across industries. The major challenges have been found to vary and some are related to the context and purpose of the applications, as different types of data and goals may lead to different concerns. The following contains breakdown across the relevant domains.

Health Usability studies of healthcare applications have seen a rise in recent years. All the studies we found examined electronic medical record (EMR) usage. Specifically, Baumann et al. [11] worked on exploring data usability challenges in health care and proposed methods in which blockchain can help address these challenges, while Gutierrez et al. [12] worked on preserving integrity in case of connectivity failure. Wenceslao et al. tried to simplify doctor-patient interaction through the use of a speech-to-text transcriber that updates this interaction to the patient's EMR. Sung et al. [13] and Lemieux et al. [14] work shows that users were concerned about privacy and were interested in blockchain applications that will give them more control over changes to their medical data.

Finance This field has received tremendous support and recognition in the blockchain space. Researchers explore existing challenges in using these applications. Voskobojnikov et al. [15] found that users were hesitant due to the absence of a regulatory body. A study by Albayati et al. [16] suggests the involvement of local government will improve the adoption rate. Alshamsi et al. [17] discovered that users viewed traditional modes of payment like credit/debit cards as more usable than bitcoins and that users believe the latter is less secure. Moniruzzaman et al. [18] compared the use of different wallets in different platforms and found that mobile wallets were more usable than desktop ones even though they are used less than the latter. Some researchers proposed methods to improve the adoption rates: Zhong et al. [19] designed visual cues to somewhat bridge the experience gap between novice and experienced cryptocurrency users and Jang et al. [20] proposed strategies like developing a mental model to improve the acceptance of blockchain applications.

Supply Chain A study by Steertegem et al. [21] found that the domain lacks real-world blockchain-based applications and the proposed ones are mostly proofs of concept. Semi-structured interviews with the people affiliated with the industries show a need for data integration across all platforms to increase the adoption of this technology. It also found that for end-consumers, resolving trust issues will provide a boost to its adoption. Valle et al. [22] performed ground theory analysis, showing that blockchain is a sustainable technology as opposed to disruptive technology. They present enablers that can foster prompt adoption, including adding proof of access based on digital signatures, using AI to manage blockchains more efficiently, standardizations of the crypto tokens used, creating data optimization services utilizing blockchain-based robotics IoT's supporting chain-of-trust, and providing customers with decision-making toolkits.

User perception of general blockchain adaptability Kumar et al. [23] interviewed top management of a technology company to understand challenges in blockchain adoption in developing countries and concluded that developing countries are more hesitant in adopting blockchain technology. Shrestha et al. [24] used a technology acceptance model with some external constructs to understand blockchain adoption among users. The author found the quality of the system as the most influential factor in positively affecting perceived usefulness and intention to use the technology. Hossain et al. [25] study the effect of graphical user interface on the usability of blockchain. The study found that similar blockchain-related tasks were faster, easier on GUI-based systems than in CLI-based systems. Overall satisfaction of users was also higher in GUI-based systems than CLI-based systems.

4.3 Findings

This subsection lists the key challenges and proposed solutions discussed in analyzed papers. It recapitulates papers discussed based on their goal/aim, methods used for data collection, and key challenges that hinder their mass adoption. The section ends with comprehensive lists of proposed solutions discussed in the papers (Tables 2 and 3).

Challenges Following are the top challenges listed out by the researchers:

- **Risk of sensitive info being exposed**: Many users feared that their sensitive information may be exposed, as was shown to be the case in studies by Lemieux et al. [14], T. van Steertegem et al.[21], Albayati et al. [16], Voskobojnikov et al. [15], S. Scuri et al. [30], and M. Daryaei et al. [31]. Researchers used other terms like "privacy breach" and "trust issues" to look at different aspects of information leakage.
- **Difficulty in using and managing the application**: Studies by Alshamsi et al. [17], Voskobojnikov et al. [15] Scuri et al. [30], Daryaei et al. [31] shows that participants felt that applications that are difficult to operate make their adoption more challenging.
- **Lack of regulations**: User participating in surveys by Baumann et al. [11], Albayati et al. [16], Alshamsi et al. [17] Daryaei et al. [31] pointed to the lack of regulations in the blockchain as another factor that contributes to their slow adoption growth.
- **Lack of non-standardization, integration, or shared platform**: Lack of shared platform or interconnectivity among organization or within an organization were

Table 2 Goal/aim of the studies

Goal/aim	Studies
Design or Implement Suggestions for adoption improvement	Almutairi et al. [26], Valle et al. [22], Zhong et al. [19], Moniruzzaman et al. [18], Hossain et al. [25], Zhong et al. [19]
Identified data usability and collection challenges	Baumann et al. [11]
Develop and/or test the application	Sung et al. [13], Almutairi et al. [26], Jang et al. [20], Abayomi-Zannu et al. [27], Moniruzzaman et al. [18], Hossain et al. [25], Kambhatla et al. [28], Zhong et al. [19], Wenceslao et al. [29]
User perception on the use of blockchain in electronic medical records	Sung et al. [13], Lemieux et al. [14], Gutierrez et al. [12], Wenceslao et al. [29]
Investigate usability and security of cryptocurrency entities	Almutairi et al. [26], Jang et al. [20], Alshamsi et al. [17], Moniruzzaman et. [18]
User perception on use of cryptocurrencies	Albayati et al. [16], Voskobojnikov et al. [15], Scuri et al. [30]
Identify and assess risk with blockchain adoption	Valle et al. [22], Voskobojnikov et al. [15], Kumar et al. [23]
User perception on adoption of blockchain	Steertegem et al. [21], Kumar et al. [23], Scuri et al. [30], Daryaei et al. [31]
Propose regulation and local government involvement	Voskobojnikov et al. [15]
Study user behavioral attitude toward the use of blockchain system	Panait et al. [32], Shrestha et al. [24], Kambhatla et al. [28]

Table 3 Methods for data collection

Method	Studies
Semi-structured interview	Steertegem et al. [21]
Heuristic evaluation	Jang et al. [20]
Cognitive walkthrough	Moniruzzaman et al. [18]
Questionnaire/survey	Sung et al. [13], Lemieux et al. [14], Albayati et al. [16], Kumar et al. [23], Panait et al. [32], Jang et al. [20], Alshamsi et al. [17], Voskobojnikov et al. [15], Abayomi-Zannu et al. [27], Scuri et al. [30], Daryaei et al. [31], Gutierrez et al. [12], Zhong et al. [19]
Observational study	Sung et al. [13], Almutairi et al. [26], Abayomi-Zannu et al. [27], Moniruzzaman et al. [18], Hossain et al. [25], Kambhatla et al. [28], Zhong et al. [19], Wenceslao et al. [29]

pointed out in research by S. Baumann et al. [11] V. L. Lemieux et al. [14] T. van Steertegem et al. [21]

- **Additional challenges**: Baumann et al. [11] identified the challenge of inability to share large sizes of data on blockchain. Steertegem et al. [21]found that scalability and governance are challenges in blockchain applications. Users feel that miners may create a centralized organization. On the other hand, study by Kumar et al. [23] suggests that this technology seems scalable and would soon witness widespread adoption. Study by Della et al. [22] points to the lack of enablers in the industry while Daryaei et al. [31] suggests volatility for its lack of adoption. Article in Statista [33] points out an interesting fact about 1 Bitcoin transaction taking 12 times more energy than 100,000 VISA transactions. This huge energy consumption directly affects the environment.

Proposed solutions for improving adoption Various solutions were discussed in the papers to increase the adoption rate of these applications.

- **Transparency**: Users participating in studies by Lemieux et al. [14], Scuri et al. [30], and Almutairi et al. [26] wanted more transparency in the internal working of the system and the cryptographic proof of applications in use.
- **Simple and Usable applications**: Studies by Almutairi et al. [26], Jang et al. [20], Daryaei et al. [31], and Moniruzzaman et al. [18] stress that simple and usable application can improve the usability, which increases their adoption.
- **Confidence and Experience**: Participants in Albayati et al. [16] and Zhong et al. [19] showed that more experienced and confident users were more likely to use and adopt newer Blockchain systems.
- **Warning against threats, awareness, and education**: Participants in studies by Almutairi et al. [26], Daryaei et al. [31], Kambhatla et al. [28] felt that there should be more awareness and education related to using Blockchain-based technology. Users also suggested deploying a warning system against possible threats to save users from any fraudulent attacks and help increase their security perception of the application.
- **Quality of Service**: Shrestha et al. [24] define quality of service as the degree to which a person is pleased, hence reducing users' psychological objection to the system or the loss of volition. The research also found that the quality of the system directly affects the intention to use the system.
- **Other proposed solutions**: Research by Lemieux et al. [14] shows that the participants desired a clear and understandable terms and conditions before continuing the use of such applications. Participants in a survey by Lemieux et al. [14] and Panait et al. [32] suggest they would prefer to have total control of their data in order to feel secure and increase such application's adoption. Albayati et al. [16] propose regulation by local government. Scuri et al. [30] propose reward system that can encourage the use of such applications.

5 Conclusion

The systematic review of the usability of blockchain-based applications shows the current research direction, challenges, and proposed solutions in the wide adoption of the technology. Top challenges hindering the adoptions are the risk of exposed sensitive information, difficulty in using the application, and lack of regulation and standardization in the industry. Proposed solutions include enhancing the transparency of the system, creating simple and usable applications, adding clear warnings against threats, and increasing awareness related to the threats and safeguards of the system.

One of the findings is that a large percentage of these usability studies include less than 40 participants, which is the minimum recommended number for a quantitative study by Neilsen [5]. As usability studies have been shown to help transition products from the prototype to the commercial stage, developing new user studies with a larger number of users can help improve the rate of real-world adoption of these applications.

Overall, this study suggests that blockchain application development is still in its infancy and that a limited number of usability research studies, especially outside the field of finance, have been carried out. This research aims to assist new researchers in developing and running new usability studies, by pointing to the current state of the research.

References

1. Triple-a (2021) Insights into cryptocurrency adoption across europe and america. https://bit.ly/3dFJK3x
2. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Decentralized Bus Rev 21260
3. Online F (2021) Number of blockchain wallet users 2021/2022: breakdowns, timelines, and predictions. https://bit.ly/3IEkZ63
4. Cryptocom (2021) Global- crypto users over 200 million. https://bit.ly/3rSQJhV
5. Nielsen J (1994) Usability engineering. Morgan Kaufmann
6. nn group (2021) Introduction to usability. https://bit.ly/3oIjDPK
7. Brooke J et al (1996) Sus-a quick and dirty usability scale. Usability Evalu Ind 189(194):4–7
8. Kitchenham B (2004) Procedures for performing systematic reviews, vol 33. Keele University, Keele, pp 1–26
9. Stewart Stute S (2019) The gender gap in patents: an exploration of bias against women in patent attainment and "blockchain" as potential remedy
10. Magas J (2020) The number of women in crypto and blockchain is skyrocketing in 2020. https://bit.ly/3lUC7uC
11. Baumann S, Stone R, Abdelall E, Srikrishnan V, Schnieders T, Fales C, Mumani A (2019) Implementing blockchain to enhance usability of patient-generated data. In: Proceedings of the human factors and ergonomics society annual meeting, vol 63, pp 1344–1348
12. Gutiérrez O, Romero G, Pérez L, Salazar A, Charris M, Wightman P (2020) Healthyblock: blockchain-based it architecture for electronic medical records resilient to connectivity failures. Int J Environ Res Public Health 17(19):7132

13. Sung M, Park S, Jung S, Lee E, Lee J, Park YR (2020) Developing a mobile app for monitoring medical record changes using blockchain: development and usability study. J Med Internet Res 22(8):e19,657
14. Lemieux VL, Hofman D, Hamouda H, Batista D, Kaur R, Pan W, Costanzo I, Regier D, Pollard S, Weymann D et al (2021) Having our "omic" cake and eating it too? Evaluating user response to using blockchain technology for private and secure health data management and sharing. Fron Blockchain 3:59
15. Voskobojnikov A, Obada-Obieh B, Huang Y, Beznosov K (2020) Surviving the cryptojungle: Perception and management of risk among north american cryptocurrency (non) users. In: International conference on financial cryptography and data security. Springer, Berlin, pp 595–614
16. Albayati H, Kim SK, Rho JJ (2020) Accepting financial transactions using blockchain technology and cryptocurrency: a customer perspective approach. Technol Soc 62(101):320
17. Alshamsi A, Andras P (2019) User perception of bitcoin usability and security across novice users. Int J Hum Comput Stud 126:94–110
18. Moniruzzaman M, Chowdhury F, Ferdous MS (2020) Examining usability issues in blockchain-based cryptocurrency wallets. In: International conference on cyber security and computer science. Springer, Berlin, pp 631–643
19. Zhong Z, Wei S, Xu Y, Zhao Y, Zhou F, Luo F, Shi R (2020) Silkviser: a visual explorer of blockchain-based cryptocurrency transaction data. In: VAST 2020, IEEE, pp 95–106
20. Jang H, Han SH, Kim JH (2020) User perspectives on blockchain technology: user-centered evaluation and design strategies for dapps. IEEE Access 8:226,213–226,223
21. Van Steertegem T, Semeijn J, Gelderman CJ (2019) Blockchain usability within supply chains: Novelty solutions and consumer benefits? In: 28th international IPSERA conference: art and science of procurement
22. Della Valle F, Oliver M (2020) Blockchain enablers for supply chains: how to boost implementation in industry. IEEE Access 8:209,699–209,716
23. Kumar R, Tahir MF, Kumar S, Zia A, Memon H, Mahmood W (2019) Challenges in adoption of blockchain in developing countries. In: 2019 4th ICEEST, IEEE, pp 1–8
24. Shrestha AK, Vassileva J (2019) User acceptance of usable blockchain-based research data sharing system: an extended tam-based study. pp 203–208
25. Hossain T, Mohiuddin T, Hasan AS, Islam MN, Hossain SA (2020) Designing and developing graphical user interface for the multichain blockchain: towards incorporating hci in blockchain. In: ISDA 2020, Springer, Berlin, pp 446–456
26. Almutairi E, Al-Megren S (2019) Usability and security analysis of the Keepkey wallet. In: 2019 IEEE ICBC, IEEE, pp 149–153
27. Abayomi-Zannu TP, Odun-Ayo I, Tatama BF, Misra S (2020) Implementing a mobile voting system utilizing blockchain technology and two-factor authentication in nigeria. In: IC4S 2019. Springer, Berlin, pp 857–872
28. Kambhatla G, Coblenz M, Oei R, Sunshine J, Aldrich J, Myers BA (2020) A pilot study of the safety and usability of the obsidian blockchain programming language. In: PLATEAU 2019, Schloss Dagstuhl
29. Wenceslao SJMC, Estuar MRJE (2019) Using cTAKES to build a simple speech transcriber plugin for an EMR. In: Proceedings of the third ICMHI 2019, pp 78–86
30. Scuri S, Tasheva G, Barros L, Nunes NJ (2019) An hci perspective on distributed ledger technologies for peer-to-peer energy trading. In: IFIP conference on human-computer interaction. Springer, Berlin, pp 91–111
31. Daryaei M, Jassbi J, Radfar R, Khamseh A (2020) Bitcoin adoption as a new technology for payment mechanism in a tourism collaborative network. In: Working conference on virtual enterprises. Springer, Berlin, pp 167–176
32. Panait AE (2020) Is the user identity perception influenced by the blockchain technology? In: 2020 IEEE international conference on intelligence and security informatics (ISI). IEEE, pp 1–3
33. de Best R (2021) Bitcoin average energy consumption per transaction compared to that of visa as of July 29, 2021. https://bit.ly/30dN0zV

Detection of Respiratory Disease Patterns Using Mask R-CNN

Eisler Aguilar, Alexandra La Cruz, Raul Albertti, Martin Carnier, Liliana Gavidia, and Erika Severeyn

Abstract The analysis and identification of pathological signs associated with different respiratory diseases are is not an easy task. One of the imaging modalities for these signs identification is examining chest CT scans. However, it requires expert knowledge to avoid human error. The purpose of this work is to implement, test, and analyze the performance of a neural network based on a mask R-CNN model able to identify some pathological signs of respiratory disease. The CT images used were manually labeled and pre-classified as positive and negative cases by specialists to prepare them for the training process. Preliminary results reached detection of ground-glass opacity with a sensitivity of 81.89% using the validation set and 92.66% using the test set. Nevertheless, low percentages were obtained for pulmonary nodules detection with a sensitivity of 51.08 and 40.34% using validation and test sets, respectively.

E. Aguilar (✉)
Department of Electronic and Circuits, Universidad Simón Bolívar, Caracas, Venezuela
e-mail: eislerandres1@gmail.com

A. La Cruz
Engineering Faculty, Universidad de Ibagué, Ibagué, Tolima, Colombia
e-mail: alexandra.lacruz@unibague.edu.co

R. Albertti · M. Carnier
Alumbra.ai, Santiago de Chile, Chile
e-mail: raulalbertti@alumbra.ai

M. Carnier
e-mail: martincarnier@alumbra.ai

L. Gavidia
Engineering, Science and Technology School, Universidad Internacional de Valencia, Valencia, Spain
e-mail: liliana.gavidia@campusviu.es

E. Severeyn
Department of Thermodynamics and Transfer Phenomena, Universidad Simón Bolívar, Caracas, Venezuela
e-mail: severeynerika@usb.ve

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_65

Keywords Neural network · Mask R-CNN · Computed tomography

1 Introduction

Misinterpretation of patterns visualized on chest computed tomography (chest CT) can lead to misdiagnosis of the disease present. These problems often occur because of problems with the CT scanner, errors in perception, reasoning, or even lack of knowledge. The study conducted in [1] shows error ranges between 10% and 25% in identifying pathological signs. It also claims that there are significant differences in terms of the level of experience of radiologists. Furthermore, approximately, 60–80% of the errors are perceptual errors. The analysis of chest CT images allows a variety of pathological signs to be observed.

Implementing an automated system for interpreting chest CT images presents an advance in medicine and speeds up the work of specialists. Currently, it is possible to design an algorithm based on a convolutional neural network (CNN) model, capable of teaching the network through a set of images with or without pathological patterns, and detect these patterns, and differentiating between a healthy and sick patient. We do not expect to obtain a specific and assertive diagnosis but to simplify healthcare by filtering patients, allowing to focus on urgent care cases, and reducing waiting times.

First, we present a revision of some patterns associated with respiratory diseases (Sect. 3). Second, the databases of chest CT images chosen for training our model are described. Then, we revised the most current CNN architectures used for object detection, and then, we chose the model that best suits the needs of this project. The selected neural network was implemented and fine-tuned to obtain the best results (Sect. 6). The results (Sect. 7) show a recall to ground-glass with 81.89 and 92.66% using validation and test sets, respectively. Meanwhile, we obtained a recall of 51.08% using validation and 40.34% test sets. Finally, Sects. 8 and 9, present the discussion, conclusions and future work respectively.

2 Patterns in Pulmonary Diseases

Several patterns associated with different respiratory can usually be extracted by analyzing a chest CT scan. These patterns come in two main groups: increased and decreased lung density. We are interested in focusing on pulmonary nodules and ground-glass opacity detection. Both of which are associated with increased lung density.

Pulmonary Nodules: Pulmonary Nand nodular opacities can be small in size (larger than 2 mm) or miliary (1–2 mm) [2]. Their distribution can be centrolobulillar, perilymphatic, and random. In particular, centrolobulillar nodules are located inside the secondary pulmonary lobe, close to the pleura, interlobar fissures, and interlobular septa. Nodules larger than 1 cm in diameter may be a cluster of small nodules.

Ground-Glass Opacity: Tarnished or ground-glass opacity is characterized by a slight increase in pulmonary attenuation that keeps bronchial and vascular contours visible [2]. This opacity can be identified if there is a partial filling of the alveoli, interstitial thickening, partial collapse of alveoli, normal respiratory status, or increased capillary flow.

3 Related Work

There are currently several architectures of CNN used for objects and patterns detection or performing image segmentation. We are interested in trying R-CNN-based architectures and RetinaNet.

Faster R-CNN [3] (2016) belongs to the region-based CNN (R-CNN) branch and is a mix of its predecessor fast R-CNN [4] and a region proposal network (RPN). The task of the RPN is to determine the relevant areas, better known as regions of interest (RoI). It is a small network that scans the last convolutional layer with anchor boxes of different dimensions, obtaining two outputs: the class (0 or 1), indicating an RoI; and the region, the corresponding coordinates of that region (Xmin, Ymin, width, height). Both fast R-CNN and faster R-CNN have the same cost function. It is possible to consider the proposed regions by RPN for the classification and detection of the desired objects or patterns. Several tests performed in [3] remark the most outstanding one is the faster R-CNN compared to its predecessor fast R-CNN.

Mask R-CNN (2018) [5] is the most current model that is part of the R-CNN family and is considered the best performing architecture. In essence, it follows the same faster R-CNN architecture but adds a new feature vital to its operation. This new feature, called a "mask," is a binary image of equal dimension to the input image, which provides the object location. The mask improves the efficiency of the network and is executed in parallel for contour box recognition. Furthermore, it also modifies the RoIPool operation proposed in fast R-CNN [4] by RoIAlign, since the former presents a mismatch between the input and the extracted feature matrix. All this, due to the misalignment of the contour box predicted by the network compared to the real one. Tests performed in [5] showed that mask R-CNN outperforms considerably faster R-CNN in contour box detection.

RetinaNet [6] uses a combination of ResNet [7] with feature pyramid network (FPN) [8] to extract image features at multiple scales without losing information in the network density. Each feature scale has two sub-networks: class and box. The innovative aspect of this model is its cost function. In [6], authors introduced a new function called "Focal Loss," which solves class imbalance problems by reducing the number of false positives. Tests performed in [6] exhibit a difference of 7.6% in AP for the most complex structure and 7.8% AP_{50} for the second-best architecture.

Mask R-CNN achieves the best result for precision, but it is the slowest model. Faster R-CNN, is the fastest model, while RetinaNet has the worst performance, although it requires less memory to work. We decided to use mask R-CNN because we want to obtain the segmentation of the pathological signs for analysis, and Mask R-CNN is the only one among the mentioned models that present this feature.

4 Datasets

MosMedData: It belongs to the Diagnostic and Telemedicine Center of the Moscow Healthcare Department, Russia. This dataset has chest CT scans in patients exhibiting symptoms of COVID-19 [9]. It has 1110 studies from different patients showing signs of ground-glass. However, as mentioned above, it is necessary to include segmentation of the findings for mask R-CNN to work with, and most of the studies in this dataset do not have it. Of the 1110 studies, only 50 included the mask. Still, the negative studies are useable for the network because they represent studies without findings and do not need any segmentation. Consequently, we only used 50 studies with ground-glass patterns and 100 studies of healthy patients. Each study has between 30 and 50 images, each with 512 × 512 resolution.

LNDb: Lung Nodule database focuses on pulmonary nodules developed by the São João Hospital and University Center in Porto, Portugal. It contains 294 studies, each representing one patient, although we use 229 studies in the project. Each study was segmented by at least one radiologist and reviewed by a maximum of three, so each has one or more masks; each one has approximately 300 images, all with a resolution of 512 × 512 [10].

5 Image Processing and Data Augmentation

Our model analyzes image by image, making it necessary to separate them with patterns (positive) and without (negative). For the LNDb dataset, we also considered the masks with the most patterns and discarded all the patterns marked as false positives by radiologists. In the case of MosMedData, we had to change the segmentation labels because all signs had the same, so we could not identify each pattern separately for training.

We also performed an image balancing by selecting fifteen (15) random images from each healthy study from MosMedData; five (5) random images with no patterns from each study with COVID-19 as well from MosMedData; ten (10) random images without patterns of each study with nodules from LNDb; and augmenting images with ground-glass using horizontal flip and rotation of random degrees (avoiding 0° , 90°, and 360°).

Finally, we distributed the images in training, validation, and test datasets in the following proportion: 70%, 20%, and 10%, respectively. We show the number of images in each of them in Table 1.

Table 1 Image balance

	Negatives	Ground-glass	Nodules	Total
Training	2828	2131	2215	7174
Validation	808	609	633	2050
Test	404	304	316	1024
Total	4040	3044	3164	10248

6 Implementation Details

We decided to use the class mask R-CNN of PyTorch to provide flexibility in choosing the hyperparameters: epochs, learning rate, weight decay, and learning rate decay, and the backbone used for training adjustments. Specifically, we used a Tesla K80 GPU and PyTorch 1.1 with CUDA 9.0 since that was the supported version for the driver GPU.

We evaluated the model performance using the confusion matrix and the metrics: precision, recall (sensitivity), and specificity. We prioritize recall because we want a model that can detect all patterns in an image, then the precision for evaluating true positive patterns, and finally, specificity (in images only) because we want to ensure that the model does not detect any pattern in negative images.

The metrics must be calculated based on the intersection over union (IoU) algorithm to ensure that the predicted pattern matches in position and label with the real one. For this reason, we have to specify a threshold that determines whether the pattern can be defined as true positive (TP) or false negative (FN).

In addition, the network may return the same pathological sign multiple times. We implement a non-maximum suppression (NMS) algorithm to mitigate this behavior and combine the repeated patterns. Therefore, we declared another threshold that indicates which patterns can be grouped. Finally, we have to define the third threshold as the minimum output score used to consider a predicted pattern present in the image. Thus, these parameters do not affect the training but can change its performance.

7 Results

We performed a first training to test the behavior of the thresholds defined above with only five (5) epochs, ResNet50-FPN backbone (pre-trained), learning rate of 0.0005, SGD optimizer with a momentum of 0.9 without weight decay, and a learning rate decay of 0.1 every three (3) epochs to check the behavior of the different metrics. Figure 1 show how the precision and sensitivity of the model vary when we modify the output score between 0.3 and 0.7, meanwhile keeping the NMS and IoU threshold at 0.3 and 0.5, respectively. For this, we obtain a peak of sensitivity with a score of 0.5.

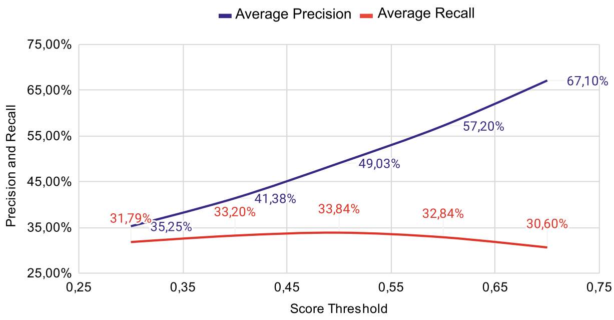


Fig. 1 Sensitivity and precision versus output score—validation dataset

Table 2 Variation of sensitivity (S) and precision (P) according to the NMS threshold

	Training		Validation		Test	
NMS	P	S	P	S	P	S
0.3	56.02	47.89	49.03	33.84	52.58	37.61
0.4	54.71	48.45	47.65	34.16	51.57	37.78
0.5	47.62	50.81	41.15	35.84	45.12	38.62
0.6	47.62	50.81	41.15	35.84	45.12	38.62

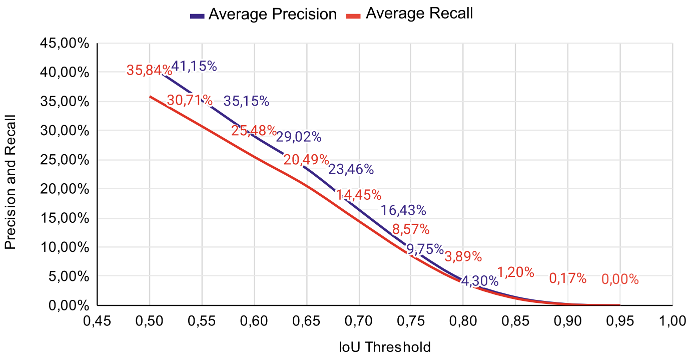


Fig. 2 Sensitivity and precision versus IoU threshold—validation dataset

Then, keeping IoU and score thresholds at 0.5 and varying the NMS threshold from 0.3 to 0.7, we also obtained the best result with an NMS threshold of 0.5 (Table 2). In this case, we can observe the results do not change after the threshold of 0.5 because no more patterns can be grouped. Finally, with an NMS and output score threshold of 0.5, we varied the IoU threshold between 0.5 and 0.95 in steps of 0.05 (Fig. 2 show the results). As the threshold requirement increases, precision and sensitivity values decrease because we demand more similarity between the prediction and the original.

Table 3 Best training results by backbone

Epochs	Backbone	LR	Opt	M	WD	Step	Gamma	B Epoch	*S* (%)	*P* (%)
20	ResNet50-FPN	0.0005	SGD	0.9	0.0005	–	–	19	47.42	54.93
10	ResNet50-FPN	0.002	SGD	0.9	0.0005	–	–	10	47.12	44.97
10	ResNet50-FPN	0.0005	SGD	0.9	0.0005	–	–	10	46.47	43.19
10	ResNet50-FPN	0.001	SGD	0.9	0.0005	–	–	10	45.02	47.96
20	ResNet50-FPN	0.0005	SGD	0.9	0.1	10	0.5	11	42.84	47.96
20	ResNet50-FPN	0.0005	SGD	0.9	0.0005	–	–	19	47.42	54.93
25	ResNet18-FPN	0.0005	SGD	0.9	0.1	–	–	15	41.55	40.82
25	VGG11	0.0005	SGD	0.9	0.0005	–	–	25	19.81	26.60
25	MobileNetv2	0.0005	SGD	0.9	0.5	–	–	14	13.58	8.88
25	AlexNet	0.0005	SGD	0.9	0.0005	–	–	25	8.82	24.55

(*S*) correspond to the sensitivity and (*P*) to the precision

Training: We applied several training sessions, varying the parameters: epochs: 5 to 30; backbone: ResNet50-FPN, ResNet18-FPN, MobileNetv2, AlexNet y VGG11; learning rate: 0.0005 to 0.002; optimizer: SGD and Adam; momemtum: 0.9 or No; weight decay: 0 to 0.5; and learning rate decay: Step: 3, 10 or No; and Gamma: 0.1, 0.5 or No. Table 3 shows the best results and the best results by backbones, respectively, with an IoU, NMS, and Output Score of 0.5. The best model corresponds to ResNet50-FPN, with a learning rate of 0.0005, SGD optimizer with momentum 0.9, and weight decay of 0.0005. Using ResNet50-FPN, we obtained a performance of ≈1.5 img/sec.

Finding Analysis: From the radiologist's perspective, we want to be able to identify whether a pathological sign, in this case, nodules or ground-glass, is present in the image and define its respective position. When radiologists make their diagnosis, they usually locate the patterns based on quadrants: upper, middle, or lower, further subdivided into the left or right lung. Therefore, regardless of the IoU threshold's value, we always ensure that the predicted pattern and the real one are in the same position, due to the IoU algorithm's behavior. So in the following tests, we compared the results of the model with an IoU threshold of 0.5 versus 0.05. On the other hand, we also compared three models: first training, best model, and last training (state of the model in its last epoch). Analyzing all data with one model, we obtained a performance of ≈3 img/sec. The best average sensitivity results obtained correspond to the best model (see Table 4) for an IoU threshold of 0.05. Note that sensitivity percentages higher than 90% are obtained for the groud-glass pattern, while for nodule it is between 35 and 40% approximately in the test set.

Table 4 Finding analysis

			Ground-Glass		Nodule	
Dataset	Model	IoU Threshold	Precision	Sensitivity	Precision	Sensitivity
Validation	First training	0.05	65.13	70.07	56.78	34.21
		0.5	36.42	39.18	39.13	23.57
	Best model	0.05	58.49	81.89	64.27	51.08
		0.5	32.43	45.41	51.07	40.52
	Last training	0.05	64.91	75.66	72.08	48.17
		0.5	39.01	45.47	51.95	34.71
Test	First training	0.05	76.70	79.22	67.80	33.52
		0.5	49.17	50.78	57.63	28.41
	Best model	0.05	69.36	92.66	58.92	40.34
		0.5	44.33	59.22	52.70	35.86
	Last training	0.05	74.83	86.41	65.10	35.31
		0.5	55.75	64.38	58.33	31.64

Table 5 Images analysis

			Ground-glass			Nodule		
Dataset	Model	IoU Threshold	*P*	*S*	*E*	*P*	*S*	*E*
Validation	First training	0.05	92.86	68.31	95.90	88.75	33.65	96.52
		0.5	86.99	35.14	95.90	84.48	23.22	96.52
	Best model	0.05	88.05	82.27	90.87	83.38	49.92	91.49
		0.5	78.41	40.56	90.87	79.81	39.34	91.49
	Las training	0.05	89.57	76.19	92.87	85.47	47.39	93.24
		0.5	82.86	42.86	92.87	80.83	33.97	93.24
Test	First training	0.05	89.45	69.74	93.64	89.00	28.16	97.10
		0.5	80.62	34.21	93.64	86.75	22.78	97.10
	Best model	0.05	88.16	88.16	90.32	77.62	35.13	91.30
		0.5	78.95	44.41	90.32	75.57	31.33	91.30
	Last training	0.05	88.72	77.63	92.19	82.76	30.38	94.65
		0.5	82.95	48.03	92.19	80.95	26.90	94.65

(*S*) correspond to sensitivity, (*P*) to precision, and (*E*) to spEcificity

Image Analysis: When we analyze the image labeling, it was necessary to modify the criteria to calculate the metrics. Therefore, we define the following: true positive (TP): at least 70% of the patterns present in the image must be detected; false positive (FP): detection in a negative image; false negative (FN): if the model does not detect any pattern in a positive image, or 70% of the findings present are not detected; and true negative (TN): no detection in negative images.

As shown in Table 5, good results are presented in the sensitivity values for images with ground-glass detection, reaching again percentages higher than 80%. We got better results using an IoU threshold of 0.05 for image with ground-glass presence. While there are no significant variations between the sensitivity of nodules with a threshold of 0.05 and 0.5.

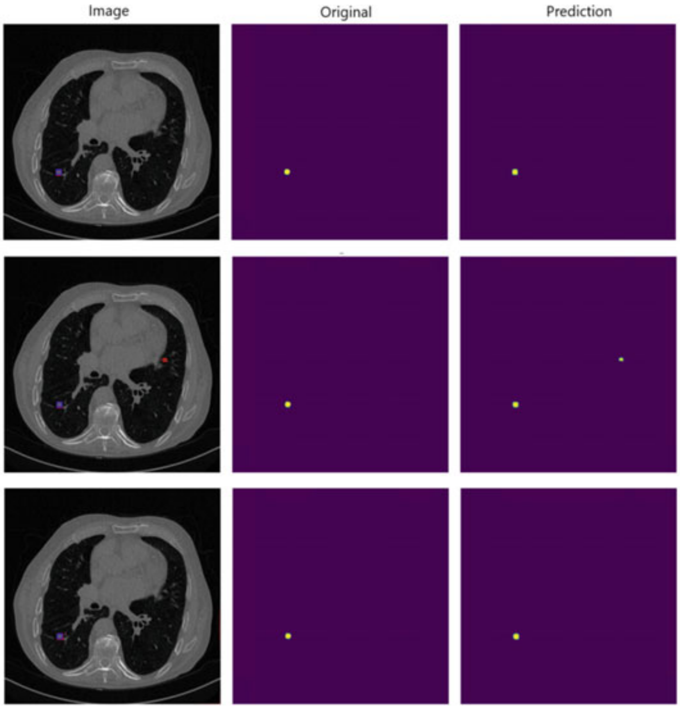


Fig. 3 LNDb: from the top to the bottom the best model—last training—first training (output score: 0.25)

Nodules: Detection of the selected image (Fig. 3) was performed correctly with the best model and the last training, with a TP and FP, while the first training did not detect anything. However, for an Output Score of 0.25, even the first training can correctly detect the image that it could not before.

Ground-Glass: On the other hand, it can be seen how the model has the ability to detect ground-glass with no difficulty. Two images were selected at random from the test dataset; both have the same detection for all test models, with slight differences between them. In particular, the image shows how the model detects patterns correctly (Fig. 4).

8 Conclusions

Generally, the final result in the specialist's report does not show the exact location of the finding, but a more generalized one. According to this, it is possible to make the evaluation criteria more flexible and support the experts. In this research, the model performance varies by modifying the analysis criteria: Output Score, NMS Thresh-

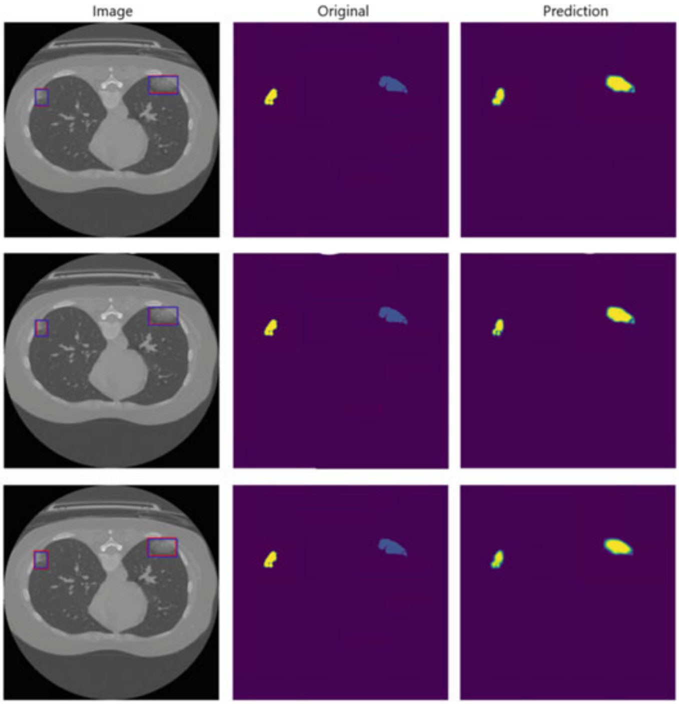


Fig. 4 MosMedData: from the top to the bottom the best model—last training—first training

old, and IoU Threshold. The sensitivity value for ground-glass detection (81.89% for validation and 92.66% for test in the analysis of findings; and 82.27% for validation and 82.16% for test in the analysis of the images) was better than for nodule detection (51.08% for validation and 40.34% for test in the analysis of the findings; and 49.92% for validation and 35.13% for test in the analysis of the images). Specificity values do not vary between an IoU Threshold of 0.5 and 0.05, obtaining results around 90–98% in all cases. This indicates that the network identifies which images are positive and negative. This aspect is of great relevance since it shows that the low sensitivity values are due to problems of the patterns localization.

Decreasing the minimum Output Score, the architecture does indeed perform detection adequately, but it decreases its ability to discriminate with a high degree of certainty among different patterns. On the other hand, low sensitivity values achieved for lung nodules were due to the low number of nodules that may be present in the same image. An image with nodules usually has at most three findings for the dataset used; therefore, even if the network detects 2 out of 3, it will not be marked as true positive as it only detected 66.67% of the findings present, since the model require 70%.

9 Future Work

Further studies are necessary to increase the amount of data used for this type of work, because it adds robustness and security to it, allowing to obtain a more generalized detection algorithm. An interesting improvement is the use of tomographic studies of the region. By working in collaboration with the medical staff, it is possible to increase the number of studies and patterns related to the region's local populations. Also, it could compare other models based on mask R-CNN or with segmentation (U-Net), or even use detection models without segmentation (RetinaNet), adding a layer for this task.

A deeper analysis of the effects of the evaluation criteria can be carried out. As could be observed, by decreasing the requirements of these parameters, better results can be obtained, but it should be validated whether the expectations of the medical team are met. Considering that the specialist only desires the location of the pattern according to its quadrant, a suggestion may be to discard the IoU threshold. Following the medical criteria, the IoU overlapping is not necessary; therefore, a different evaluation criterion can be designed that only ensures that both the predicted pattern and the original pattern are in the same area of the image. Also, it is possible to lower the scoring requirement only for nodules, then try their performance with this criterion; it is even possible to evaluate the effect of decreasing this parameter for both patterns.

References

1. Taleno DA (2017, September) Signos Radiológicos en Tomografía y Resonancia Magnética y Grado de Conocimiento de los Residentes de Radiología, en Pacientes atendidos en HEALF, Octubre 2013–2014," Master's thesis, Universidad Nacional Autónoma de Nicaragua, Managua, Nicaragua
2. Franquet T (2012) Diagnóstico por imagen de las enfermedades pulmonares difusas: Signos y patrones diagnósticos básicos. Medicina Respiratoria 5(3):49–67
3. Ren S, He K, Girshick R, Sun J (2015) Faster R-CNN: towards real-time object detection with region proposal networks. In: Proceedings of the 28th international conference on neural information processing systems, vol 1, NIPS'15. MIT Press, Cambridge, MA, USA, pp 91–99
4. Girshick R (2015, December) Fast r-cnn. In: Proceedings of the IEEE international conference on computer vision (ICCV)
5. He K, Gkioxari G, Dollár P, Girshick R (2017) Mask r-cnn. In: 2017 IEEE international conference on computer vision (ICCV)
6. Lin T-Y, Goyal P, Girshick R, He K, Dollár P (2017) Focal loss for dense object detection. In: 2017 IEEE international conference on computer vision (ICCV)
7. He K, Zhang X, Ren S, Sun J (2016) Deep residual learning for image recognition. In: 2016 IEEE conference on computer vision and pattern recognition (CVPR), pp 770–778
8. Lin T-Y, Dollár P, Girshick R, He K, Hariharan B, Belongie S (2017) Feature pyramid networks for object detection. In: 2017 IEEE conference on computer vision and pattern recognition (CVPR)
9. Morozov SP, Andreychenko AE, Blokhin IA, Gelezhe PB, Gonchar AP, Nikolaev AE, Pavlov NA, Chernina VY, Gombolevskiy VA (2020) MosMedData: data set of 1110 chest CT scans performed during the COVID-19 epidemic. Digital Diagn 1(1):49–59

10. Pedrosa J, Aresta G, Ferreira C, Atwal G, Phoulady HA, Chen X, Chen R, Li J, Wang L, Galdran A, Bouchachia H, Kaluva KC, Vaidhya K, Chunduru A, Tarai S, Nadimpalli SPP, Vaidya S, Kim I, Rassadin A, Tian Z, Sun Z, Jia Y, Men X, Ramos I, Cunha A, Campilho A (2021) LNDb challenge on automatic lung cancer patient management. Med Image Anal 70

Efficient Support Vector Machine Toward Medical Data Processing

Guang Shi, Zheng Chen, and Renyuan Zhang

Abstract This work explores the efficient and practical scheme of medical data analysis through machine learning algorithms. The support vector machine (SVM) mechanism is specifically employed for building an artificial intelligence (AI) assistant diagnosis systems. Considering the practical demands on clinical diagnosis, the plain SVM algorithm is hardly used since the poor number of classes (typically, two classes) and explosion of samples. Therefore, a sample domain description technology is developed to realize a one-class SVM for flexibly expending the number of classes. Furthermore, a constantly online learning strategy is proposed to implement high-performance classification/diagnosis with greatly reduced database. For proof-of-concept, several medical databases are employed for diagnosis test. From the test results, the diagnosis correct rate is improved with compact database; and the scale of database is reduced while the similar correct rate is achieved by plain SVM algorithm. Maintaining the best accuracy, the proposed online learning SVM reduces the numbers of active samples (support vectors) to 23.4%, 54.6%, 70.9% of the plain for diagnosing the breast cancer, diabetes, and liver disorders, respectively, where the best accuracy is superior or similar to state-of-the-arts.

Keywords SVM · Online learning · Data domain description · Medical data

1 Introduction

The artificial intelligence (AI) has been reaching the boom and applied in various fields in past decades [1, 8]. As one of most important aspects of AI, the machine learning technology is considered as the powerful tool to analyze big data and assist

G. Shi (✉) · Z. Chen · R. Zhang
Nara Institute of Science and Technology, Ikoma, Nara, Japan
e-mail: shi.guang.rw4@is.naist.jp

Z. Chen
e-mail: chen.zheng.bn1@is.naist.jp

R. Zhang
e-mail: rzhang@is.naist.jp

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_66

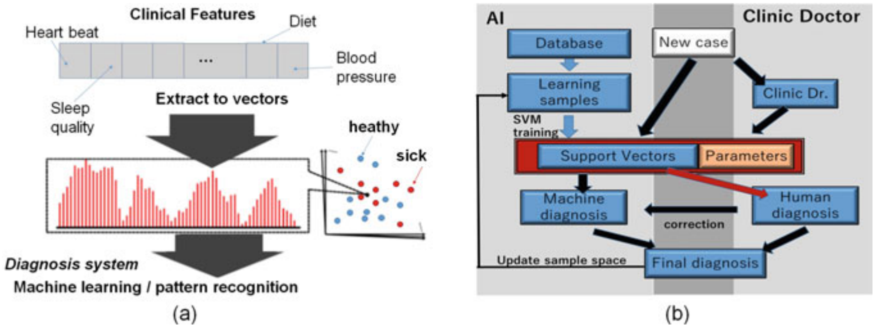


Fig. 1 **a** The medical cases are presented by the feature vectors with medical index and analyzed by information technologies; and **b** an AI diagnosis assistant system is expected through machine learning such as SVM

human to solve complex problems in real-world. For instance, many remarkable works have been reported to apply machine learning technologies in the medical science such as disease diagnosis systems [3, 5, 18]. Since most of diagnosis systems are built through data classification or so-called pattern recognition networks, this work focuses on an advanced classification algorithm support vector machine (SVM) [6, 10] in particular. From some laboratory works in medical science, SVM performs very high correct rate in categorizing medical cases which is described by the high-dimensional feature vectors [15, 17, 20]. Employing a sufficiently large database of disease cases with correct labels, SVM classifiers are built by training process. Then, the well-trained classifier accepts new cases of which the category labels are unknown (“ill” or “healthy” for instances). The classifier, known as diagnosis system, gives the predicted labels instead of clinical doctors’ judge for many diseases such as cancers [19], diabetes [16], and liver disorders [7].

From the machine learning point of view, the accurate classification is not extremely challenging if the medical data is well offered. However, the reality is that no any clinical doctor makes critical judgment through AI instead of his/her expertise knowledge. Namely, what we really need is not a diagnosis system but a diagnosis assistant system. In this exploration, an SVM diagnosis assistant system is proposed for disease status categorization as illustrated in Fig. 1. The principle of proposed SVM assistant system is offering the active samples or key cases (known as support vectors) to the clinical doctors instead of the straightforward machine diagnosis results. Namely, the number of support vectors is expected to be reduced with reasonably high accuracy.

In this paper, two strategies are proposed to achieve high-quality SVM classifications with reduced samples for two different types of application fields. To realize the multiclass SVM classification, the data domain description (DDD) algorithm on the basis of SVM is developed instead of conventional binary tree or “one-v. s. -others” strategies [2, 11, 14]. A toy example with six classes (see the “glass” dataset of UCI database [9]) is validated by the proposed SVM-DDD. The number

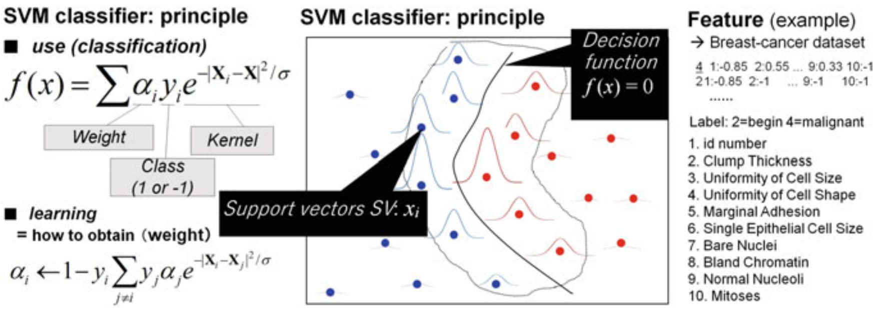

SVM classifier: principle
use (classification)
$f(x)=\sum\alpha_i y_i e^{-|\mathbf{X}_i-\mathbf{X}|^2/\sigma}$
Weight
Kernel
Class
(1 or -1)
learning
= how to obtain (weight)
$\alpha_i \leftarrow 1-y_i\sum_{j\neq i} y_j\alpha_j e^{-|\mathbf{X}_i-\mathbf{X}_j|^2/\sigma}$
SVM classifier: principle
Decision function $f(x)=0$
Support vectors SV: x_i
Feature (example)
→ Breast-cancer dataset
4 1:-0.85 2:0.55 ... 9:0.33 10:-1
21:-0.85 2:-1 ... 9:-1 10:-1
......
Label: 2=begin 4=malignant
1. id number
2. Clump Thickness
3. Uniformity of Cell Size
4. Uniformity of Cell Shape
5. Marginal Adhesion
6. Single Epithelial Cell Size
7. Bare Nuclei
8. Bland Chromatin
9. Normal Nucleoli
10. Mitoses

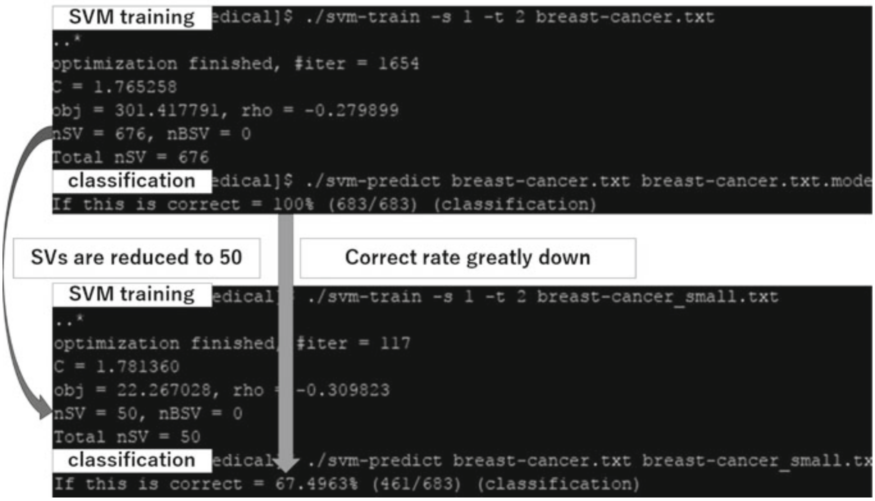
Fig. 2 Medical data is classified by SVM along with an example of breast cancer dataset

of support vectors (SVs) is reduced to 8% with even higher accuracy compared to conventional multiclass SVM powered by LIBSVM [4]. In the medical applications with dynamical and unpredictable database, a constantly online learning SVM is also proposed to achieve high accuracy and fewer active samples. The essence of this online scheme is to evaluate the significance of all the survivals (seen as SVs); and remove one insignificant SV for recruiting a new one online. Compared to the conventional incremental online SVM [12, 13], the constantly online scheme helps to keep the small size of SV pool. The breast cancer, diabetes, and liver disorders dataset from UCI database [9] are introduced for validation.With the superior or similar accuracy of state-of-the-art works, the number of SVs are reduced to 23.4%, 54.6%, 70.9% of plain SVM, respectively.

2 SVM for Medical Classification: Principle and Example

Similarly to many reported works, the SVM algorithm [6, 10] can be applied to classify a highly dimensional vector $\mathbb{X}$s with the form of $\mathbb{X} = (x_1, x_2, \ldots, x_n)$. When this vector represents the feature of a medical case, the classification label can be considered as an AI diagnosis result. The process to obtain a suitable math-model for the classification is called "SVM training process," which is out of this thesis summary. The principle of SVM training and classification is shown in Fig. 2 along with an example of breast cancer database [9]. In this example, the 689 cases of real breast cancer features are introduced with ten dimensions, and labeled by "2" as begin and "4" as malignant. The conventional SVM algorithm with Gaussian kernels is employed to pursue the prediction model from the database. The prediction function is given by:

$$f(\mathbb{X}) = \text{sign}[\sum_{i=1}^{N} \alpha_i y_i K(\mathbb{X}, \mathbb{X}_i) + b], \tag{1}$$



```
edical]$ ./svm-train -s 1 -t 2 breast-cancer.txt
..*
optimization finished, #iter = 1654
C = 1.765258
obj = 301.417791, rho = -0.279899
nSV = 676, nBSV = 0
Total nSV = 676
edical]$ ./svm-predict breast-cancer.txt breast-cancer.txt.mode
If this is correct = 100% (683/683) (classification)
```

```
edical] ./svm-train -s 1 -t 2 breast-cancer_small.txt
..*
optimization finished, #iter = 117
C = 1.781360
obj = 22.267028, rho = -0.309823
nSV = 50, nBSV = 0
Total nSV = 50
edical ./svm-predict breast-cancer.txt breast-cancer_small.tx
If this is correct = 67.4963% (461/683) (classification)
```

Fig. 3 Conventional SVM is applied for breast cancer diagnosis. When number support vectors is reduced, accuracy is going poor

where the $\mathbb{X}_i$ is the support vectors, which are selected from the database through SVM training:

$$\alpha_i \leftarrow 1 - y_i\Big(\sum_{j(\neq i)} \alpha_j y_j K(\mathbb{X}_i, \mathbb{X}_j) + b\Big). \tag{2}$$

The conventional SVM is applied to diagnose the breast cancer (see Fig. 3). When the number of support vectors (SVs) is close to entire database, the accuracy is perfect; however, when the number of SVs is smaller, the accuracy is going very poor. As mentioned above, the goal of AI diagnosis assistant system is not AI diagnosing but offering SVs (known as important reference cases) to doctors. A large number of SVs is impossible for doctors to review on site for any specific patient. Thus, conventional SVM can not be directly applied in clinic even though many works claimed that very high accuracy can be achieved by a huge database and complex math-model.

From the previous experiments, two critical issues are found in the medical data analysis by SVM:

1. Conventional SVMs are typically developed for two-class classification. However, the clinical diagnosis tasks always require more than two classes (sometimes even single class);
2. the number of SVs are expected to be greatly reduced. The classification accuracy is expected to keep in high level on the other hand.

Addressing these two issues, a data domain description technology@ @ @ [addressing issue (1)] and decremental online learning strategy [(addressing issue (2)] are proposed as follows.

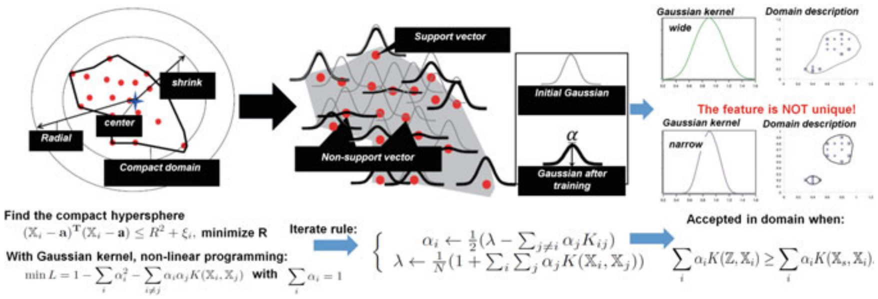

shrink
center
Radial
Compact domain
Support vector
Non-support vector
Initial Gaussian
α
Gaussian after training
Gaussian kernel
wide
Domain description
The feature is NOT unique!
Gaussian kernel
narrow
Domain description
Find the compact hypersphere
$(\mathbb{X}_i - \mathbf{a})^{\mathrm{T}}(\mathbb{X}_i - \mathbf{a}) \leq R^2 + \xi_i$, minimize R
With Gaussian kernel, non-linear programming:
$\min L = 1 - \sum_i \alpha_i^2 - \sum_{i \neq j} \alpha_i \alpha_j K(\mathbb{X}_i, \mathbb{X}_j)$ with $\sum_i \alpha_i = 1$
Iterate rule:
$\alpha_i \leftarrow \frac{1}{2}(\lambda - \sum_{j \neq i} \alpha_j K_{ij})$
$\lambda \leftarrow \frac{1}{N}(1 + \sum_i \sum_j \alpha_j K(\mathbb{X}_i, \mathbb{X}_j))$
Accepted in domain when:
$\sum_i \alpha_i K(\mathbb{Z}, \mathbb{X}_i) \geq \sum_i \alpha_i K(\mathbb{X}_s, \mathbb{X}_i)$

Fig. 4 Principle of proposed data domain description through SVM

3 Data Domain Description Through SVM

Many strategies for building multiclass SVM have been developed so far. However, in medical science (more typically, diagnosis), the number of classes is flexible even unpredictable. Thus, we are seeking a method to describe the data domain for one single class of dataset; then, the flexible-class classification will be easily realized by assembling necessary data domain description (DDD). In this work, we prefer to apply SVM-based theory for this purpose.

We try to find a sphere with minimum volume R as shown in Fig. 4, containing all (or most of) the data objects, which is defined by:

$$F(R, \mathbf{a}, \xi_i) = R^2 + C \sum_i \xi_i, \tag{3}$$

where $\mathbf{a}$ is the center of this sphere; ξ_i is a slack variable for error tolerance; and parameter C gives the trade-off between simplicity (or volume of the sphere) and the number of errors (number of target objects rejected). This function has to be minimized under the constraints:

$$(\mathbb{X}_i - \mathbf{a})^{\mathbf{T}}(\mathbb{X}_i - \mathbf{a}) \leq R^2 + \xi_i. \tag{4}$$

The accept/reject condition of object $\mathbb{Z}$ can be given by (where "accept" indicates the model correctly approve a specific test sample into its data domain; and "reject" indicates a specific sample is correctly rejected):

$$\sum_i \alpha_i K(\mathbb{Z}, \mathbb{X}_i) \geq \sum_i \alpha_i K(\mathbb{X}_s, \mathbb{X}_i), \tag{5}$$

where K is the Gaussian kernel function. By applying the SVM theory, the task becomes the following quadratic programming (QP) problem:

Table 1 A real-world dataset ("glass" from UCI database) with six classes is introduced for testing

	DDD			LIBSVM [4]	
gamma	SVs	Accept (%)	Reject (%)	SVs	Correct (%)
2	14	82.76	100	175	79.9
1	11	86.21	98.38	174	77.6
0.5	8	82.70	82.76	184	75.23
0.2	7	86.21	78.38	193	67.76
0.05	7	89.66	79.43	206	58.41

$$\min L = 1 - \sum_i \alpha_i^2 - \alpha_i \alpha_j K(\mathbb{X}_i, \mathbb{X}_j), \tag{6}$$

under the constraints: $\sum_i \alpha_i = 1$, and $0 \leq \alpha_i \leq C$. In order to solve this QP problem, another Lagrangian function is constructed with multiplier λ:

$$\begin{array}{c} \mathfrak{L} = L + \lambda(\sum_i \alpha_i - 1) \\ = 1 - \sum_i \alpha_i^2 - \sum_{i \neq j} \alpha_i \alpha_j K(\mathbb{X}_i, \mathbb{X}_j) + \lambda(\sum_i \alpha_i - 1) \end{array}. \tag{7}$$

We propose the training process as:

$$\begin{cases} \alpha_i \leftarrow \max(0, \min(\frac{1}{2}(\lambda - \sum\limits_{j \neq i} \alpha_j K_{ij}), C)) \\ \lambda \leftarrow \max(0, \frac{1}{N}(1 + \sum_i \sum\limits_j \alpha_j K(\mathbb{X}_i, \mathbb{X}_j))) \end{cases}. \tag{8}$$

For proof-of-concept, a dataset with six classes (glass dataset from UCI database) are introduced for testing. In this experiment, we select the class labeled "7" as domain describe target. The multiclass SVM by LIBSVM [4] is also implemented for comparison. The results are shown in Table 1. In our proposal, the domain feature is flexible by changing the parameter "gamma." From this example, it is found the average correct rate of our proposal could be higher than conventional SVM with greatly reduced number of SVs.

4 Online Learning SVM for Diagnosis Assistant System

In the real-world application of SVMs, the number of learning samples is usually very large and unpredictable. As a result, large database or traditional online incrementally learning strategies can be hardly implemented in the clinical diagnosis assistant systems. Fortunately, in SVM theory, some of the learning samples (non-support vectors) are ineffective, which can be removed from sample space. A "doctor-friendly"

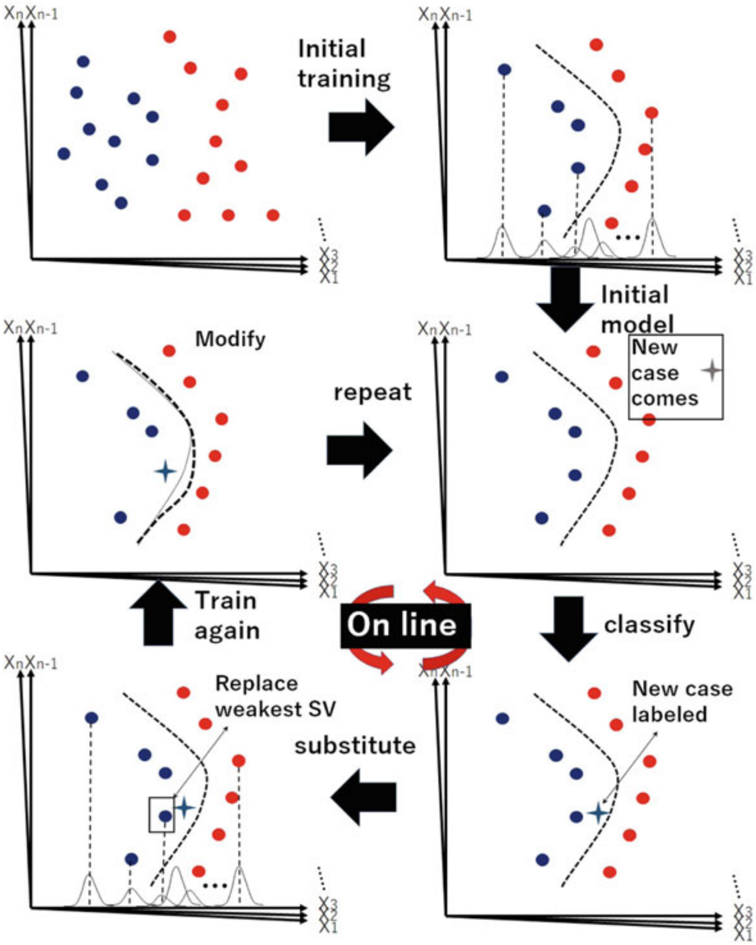


Fig. 5 Principle of proposed online learning SVM strategy

online learning strategy with constant number of learning samples is proposed in this work. In order to reduce the loss of accuracy, the effectiveness of each sample is evaluated, and only the most ineffective sample is replaced by an online pattern. In this manner, the learning sample space can be expanded within compact SV space (see Fig. 5). The process of this online learning strategy is shown as follows:

1. Initial SVM learning according to a small set of samples;
2. Classifying the new-received online pattern;
3. Evaluating the effectiveness of previous samples and replacing the most inefficient one by new-received pattern;
4. SVM learning according to the updated samples;
5. Receiving new online pattern and repeating 2, 3, and 4.

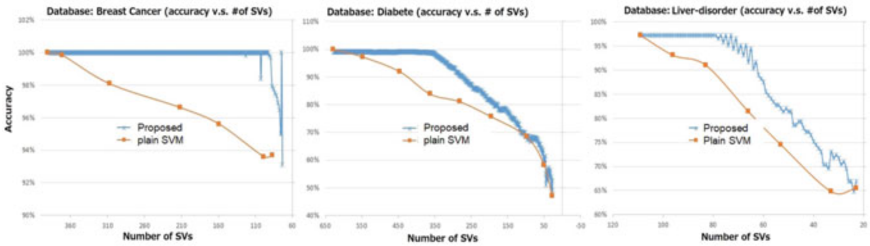


Fig. 6 Online learning SVM results for three examples: breast cancer, diabetes, and liver disorder database

After sufficient online learning operations, all the inefficient samples are replaced by significant online patterns. Then, the small scale of SVs are offered to the doctor for reviewing and referencing. This SV space is dynamically updated along with the career of specific doctors.

From the results of Fig. 6, it is obviously found the proposed constantly online SVM achieves higher correct rate when the same (reduced) scale of database is applied by conventional SVM. Namely, the minimum necessary number of SVs is reduced with the same consideration of correct rate. Making breast cancer as example: the proposed online SVM achieves perfect correct rate when the number of SVs is 89; for the same correct rate, the conventional SVM needs at least 382 SVs. Other experiments reflect similar property of the proposed online learning process. On the other hand, it is possible to simply reduce the SVs (by tuning the parameter of kernel functions, for example, but out of the scope here) with plain SVMs. However, this reduction leads the great loss of accuracy as shown in Fig. 6.

A general comparison among several types of SVM-based diagnosis is seen in Table 2. Three examples of breast cancer, diabetes, and liver disorder are validated.

Table 2 Comparisons among various SVM-based diagnosis for breast cancer, diabetes, and liver disorder

		[19]	[16]	[7]	This work	
Breast cancer	Algo.	Ensemble SVM	–	–	Plain SVM	Online
	# of samples	273	–	–	683	683
	# of SVs	N/A	–	–	382 / 89	89
	Acc.	95.43%	–	–	100%/93.8%	100%
Diabetes	Algo.	–	Plain SVM	–	Plain SVM	online
	# of samples	–	400	–	768	768
	# of SVs	–	N/A	–	635/347	347
	Acc.	–	95.36%	–	100%/82.6%	99.3%
Liver disorder	Algo.	–	–	CSA-SVM	Plain SVM	Online
	# of samples	–	–	583	145	145
	# of SVs	–	–	N/A	110/78	78
	Acc.	–	–	99.49%	97.3%/89.6%	97.3%

Since tasks are not extremely challenging in the sense of machine learning, our plain SVM classifier achieves quite similar accuracy to other SVM-based algorithms. Using the proposed constantly online learning scheme, the accuracy is maintained when the number of SVs is reasonably reduced, which is obviously better than the plain SVM by simply reducing the SVs to the same amount.

5 Conclusion

This paper investigates how to efficiently use the database through machine learning for medical data analysis. An AI diagnosis assistant system is proposed employing support vector machine. Several real-world medical databases are introduced by conventional SVM classification tests. In order to extend the number of classes and reduce the number of SVs, the data domain description algorithm and a constantly online learning strategy are developed and verified by the databases of breast cancer, diabetes, and liver disorder. From the experiments, the proposed methods are helpful to flexibly increase classes and reduce SVs with high correct rate. This diagnosis assistant system offers clinic doctor a reasonable number of SVs (known as important cases for reviewing and referencing) instead of a simple machine diagnosis result. Therefore, it is practical in clinical exercises.

References

1. Aishath Murshida A, Chaithra BK, Nishmitha B, Pallavi PB, Raghavendra S, Mahesh Prasanna K (2019, May) Survey on artificial intelligence. Int J Comput Sci Eng 7:1778–1790
2. Alam J, Alam S, Hossan A (2018) Multi-stage lung cancer detection and prediction using multi-class svm classifie. In: 2018 international conference on computer, communication, chemical, material and electronic engineering (IC4ME2) 1–4
3. Buch V, Ahmed I, Maruthappu M (2018, March) Artificial intelligence in medicine: current trends and future possibilities. Br J Gen Prac 68:143–144
4. Chang CC, Lin CJ (2011) Libsvm: a library for support vector machines. ACM Trans Intell Syst Technol (TIST) 2(3):1–27
5. Chen Z, Salazar E, Marple K, Das SR, Amin A, Cheeran D, Tamil LS, Gupta G (2018) An AI-based heart failure treatment adviser system. IEEE J Transl Eng Health Med 6:1–10
6. Cortes C, Vapnik V (1995) Support-vector networks. Mach Learn 20(3):273–297
7. Devikanniga D, Ramu A, Haldorai A (2020, April) Efficient diagnosis of liver disease using support vector machine optimized with crows search algorithm. EAI Endorsed Trans Energy Web 7:29
8. DoÅilovi FK, Bri M, Hlupi N (2018) Explainable artificial intelligence: a survey. In: 2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO), pp 0210–0215
9. Dua D, Graff C (2017) UCI machine learning repository (2017). https://archive.ics.uci.edu/ml/index.php
10. Evgeniou T, Pontil M (2001) Support vector machines: theory and applications. 2049:249–257
11. Franc V, Hlavac V (2002) Multi-class support vector machine. 2:236–239. https://ieeexplore.ieee.org/document/1048282

12. Gu B, Sheng VS (2013) Feasibility and finite convergence analysis for accurate on-line ν-support vector machine. IEEE Trans Neural Netw Learn Syst 24(8):1304–1315
13. Gu B, Sheng VS, Tay KY, Romano W, Li S (2015) Incremental support vector learning for ordinal regression. IEEE Trans Neural Netw Learn Syst 26(7):1403–1416
14. Han S, You W, Li H (2007) Application of binary tree multi-class classification algorithm based on svm in shift decision for engineering vehicle. In: 2007 IEEE international conference on control and automatio, pp 1833–1836
15. Janardhanan P, Heena L, Sabika F (2015) Effectiveness of support vector machines in medical data mining. J Commun Softw Syst 11:25–30
16. Jegan C (2013) Classification of diabetes disease using support vector machine. Int J Eng Res Appl 3:1797 – 1801
17. Jiang Y, Li Z, Zhang L, Sun P (2007) An improved SVM classifier for medical image classification. In: Kryszkiewicz M, Peters JF, Rybinski H, Skowron A (eds) Rough Sets Intell Syst Paradigms. Heidelberg, Springer, Berlin Heidelberg, Berlin, pp 764–773
18. Panayides AS, Amini A, Filipovic ND, Sharma A, Tsaftaris SA, Young A, Foran D, Do N, Golemati S, Kurc T, Huang K, Nikita KS, Veasey BP, Zervakis M, Saltz JH, Pattichis CS (2020) Ai in medical imaging informatics: current challenges and future directions. IEEE J Biomed Health Inf 24(7):1837–1857
19. Sewak M, Vaidya P, Chan CC, Duan ZH (2007) SVM approach to breast cancer classification. In: Second international multi-symposiums on computer and computational sciences (IMSCCS 2007), pp 32–37
20. Zhu H, Liu X, Lu R, Li H (2017) Efficient and privacy-preserving online medical prediagnosis framework using nonlinear SVM. IEEE J Biomed Health Inf 21(3):838–850

Geometric and Physical Building Representation and Occupant's Movement Models for Fire Building Evacuation Simulation

Joaquim Neto, A. J. Morais, Ramiro Gonçalves, and António Leça Coelho

Abstract Building evacuation simulation allows for a better assessment of fire safety conditions in existing buildings, which is why it is of interest to develop an easy-to-use Web platform that helps fire safety technicians in this assessment. To achieve this goal, the geometric and physical representation of the building and installed fire safety devices are necessary, as well as the modelling of occupant movement. Although these are widely studied areas, in this paper, we present two new model approaches, either for the physical and geometric representation of a building or for the occupant's movement simulation, during a building evacuation process. To test both models, we develop a multi-agent Web simulator platform. The tests carried out show the suitability of the model approaches herein presented.

Keywords Building evacuation · Cellular automata · Modelling occupants movement · Building representation model · Multi-agent systems

1 Introduction

The research in the fire building evacuation domain has seen significant developments in the last few decades, particularly concerning the occupants' movement's

J. Neto (✉) · A. J. Morais
Universidade Aberta, Lisboa, Portugal
e-mail: jfn@lnec.pt

A. J. Morais
e-mail: jorge.Morais@uab.pt

J. Neto · A. L. Coelho
Laboratório Nacional de Engenharia Civil, Lisboa, Portugal
e-mail: alcoelho@lnec.pt

A. J. Morais
LIAAD—INESC TEC, Porto, Portugal

R. Gonçalves
UTAD (Universidade de Trás-os-Montes e Alto Douro), Vila Real, Portugal
e-mail: ramiro@utad.pt

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_67

modelling and simulation. The researcher's main objectives are to understand the occupants' behaviour to improve buildings' design and construction, making them more effective in evacuating their occupants to a safe place. In addition, analysing fire safety conditions in buildings can help technicians define the design solutions, considering the various factors impacting fire safety. However, for this analysis to be sufficiently reliable, it is necessary to model buildings with appreciable rigour from a geometric and physical perspective and model the occupant's movement while leaving the building.

The present research work's motivation falls within the scope of our ongoing PhD thesis, which proposes a multi-agent recommender system for real-time guiding the occupants to a safe place [1]. The research in the area of fire buildings evacuation has seen significant developments in recent decades, particularly concerning the modelling and simulating of the occupant's movement. However, the modelling component related to people's behaviour under a fire emergency has not kept up with this development. Modelling the occupant's behaviour is complex and challenging due to contextual, personal and cultural factors that vary from country to country and are difficult to know and model. Even some new approaches that have been used, such as the case of serious games [2], to create sufficiently immersive environments for the potential "players", have not had the desired results yet. Thus, it is difficult to model the occupant's behaviour accurately in an emergency, becoming even more complex in later stages of fire development. In our doctoral work, we propose a paradigm shift. Instead of focusing on the occupant's behaviour, we focus on conditioning that behaviour, transmitting real-time information about the most appropriate evacuation route to the occupants. This approach makes people's behaviour more predictable, reducing the uncertainty that their behaviour introduces during the building evacuation and, thus, reducing the evacuation time, increasing the safety of buildings. In their paper, [3] present a model for analysing fire safety conditions in buildings, that besides the geometric representation of a building, also considers all the impacting factors in fire safety by integrating different simulation models, namely: fire spread; building evacuation; the response of passive and active resources and firefighters intervention.

This paper aims to present a new model for building's physical and geometric representation and a new building evacuation model regarding the occupants' movement simulation.

Section 2 introduces the problem statement and the related work; Sect. 3 presents the building representation and the occupant's movement models; Sect. 4 presents the experimental scenarios and the results. Then, Sect. 5 discusses the result. Finally, in Sect. 6, we write the research work conclusions.

2 Related Work

Analysing 22 evacuation models, [4] consider three different approach models to deal with the occupant's problem in evacuating a building. First, optimisation models treat the occupants as a whole without taking individual behaviour into account. Second, simulation models intend to represent the behaviour and movement of the occupant while evacuating. Finally, risk assessment models seek to identify hazards and the risk of an evacuation resulting from a fire or other incident type.

The literature review developed by Hamacher and Tjandra [5] analyses models and algorithms applicable to the building evacuation problem. The authors distinguish between microscopic and macroscopic evacuation models. Microscopic models are based on simulation and can model the occupants' characteristics and interactions that influence their movement. Macroscopic models do not consider individual behaviours during evacuation and use optimisation algorithms.

Besides macroscopic versus microscopic classification, models can also be classified as discrete, as is the case with the cellular automata model, or continuous as the model based on fluid-dynamic, or a combination of both [6]. The same authors also classify the models accordingly to the interaction between people: based on rules, in which people make decisions according to their situation at the moment, their neighbourhood and their goals; or force-based models, which treat interactions at the level of motion equations, similar to classical mechanics. Finally, [6] considers that the pedestrian dynamics movement can be: stochastic, based on probabilistic functions that control the behaviour, so that pedestrians can react differently to identical situations, or deterministic, in which the past determines future behaviour. Also dividing the models into macroscopic and microscopic, [7] presents a survey on models, algorithms, applications and implementations in the area of building evacuation. The author highlights the advantages and disadvantages of the analysed models, referring to the difficulty of establishing consensus in comparing their performances.

In their literature reviews, [8, 9] emphasise the importance of understanding human behaviour in the design and construction of buildings, considering that the occupants' behaviour interacts with the surroundings and, in particular, with the security measures implemented. The authors highlight the importance of identifying the behavioural factors that influence the building's evacuation process, the knowledge of the purpose of the building and the occupants' knowledge of it.

3 Building Representation and Occupant's Movement Models

In this section, we describe in detail a new model for the physical and geometric representation of a building and a new model for simulating the movement of occupants during a building evacuation process. The building representation approach allows to easily model all the geometric and physical characteristics of the building and other devices that support and assist occupants in an evacuation process in a fire. Based on that model, we also developed a new model to simulate the movement of occupants.

3.1 Building Representation Model

The building representation model is supported on a matrix where the cells result from the decomposition of the building floor plans. These cells are in the form of quadrilaterals of dimensions defined by the Web platform user. The right side of Fig. 1 shows the floor plan's decomposition of the left side figure and considers 14 cells for the floor's geometric representation. We follow the notation c_{ij} to refer to a specific cell of line i and column j.

As referred by Leça Coelho and Neto [10], besides the building's geometric representation, the platform allows defining the materials used in the building's construction and fire safety devices, such as fire detector sensors and emergency guiding signage. It is also possible to define other parameters, such as the floor's height, the type of activity developed in the building, which influences fire development (slow, moderate, fast and ultra-fast fire) and ventilation conditions. The model also allows the identification of windows, doorways with or without doors. Concerning doors characterisation, besides their size, it is also possible to define their fire resistance time, which indirectly reflects the type of material they are made.

The characterisation of each side of the elementary cells gives a geometric shape to the building. For each side of a cell, it is possible to define one of the following three types: fictitious side, which means that there is no wall and therefore it is traversable by the occupant; real interior side, to represent the interior walls, and real exterior side, to represent the exterior walls of the building. In addition, the windows and doorways are associated with the sides of the cells. Figure 2 exemplifies the characterisation of a cell using c_{22} and c_{23}.

After transforming each space into a set of elementary cells, the next step that needs to be taken to model the occupants' movement is to determine the paths they can use to exit the building. To achieve this, we will transform the cells' representation presented in Fig. 1 into a node network, to which the graph theory can be applied.(Fig. 2)

When transforming the floor plan into a node network, each cell and doorway are represented by its geometric centre, as shown on the left side of Fig. 3 The graph nodes correspond to the free cells inside the building. The outer cells of the building, adjacent to exit doorways, are also transformed into nodes, as they are the safe cells

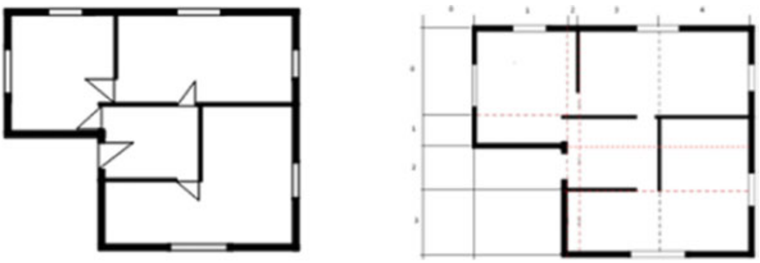


Fig. 1 Floor plan (left). Floor plan decomposed into elementary cells (right)

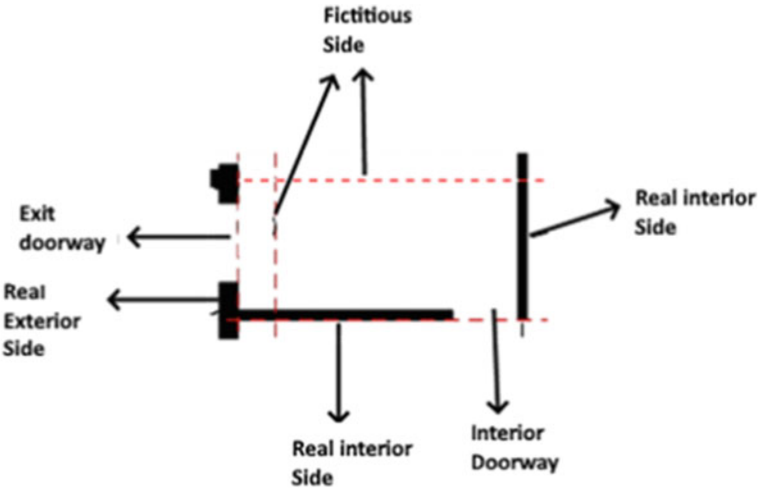


Fig. 2 Elementary cell sides characterisation

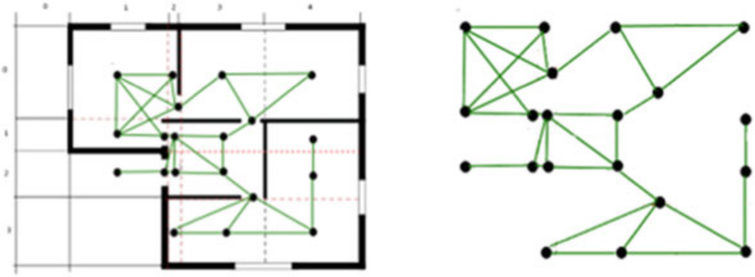


Fig. 3 Transforming a floor plan into a node network

that the occupants seek in their process of evacuating the building, as is the case of cell m_{21}.

The graph's edges result from the connection between adjacent nodes and represent the occupants' paths to exit the building. The distance between the nodes is the weight of each edge, as shown on the right side of Fig. 3. Finding the shortest path between any two nodes is possible with that weighted graph, as is the case with the problem we are addressing in the present work.

3.2 *Modelling Occupant's Movement*

As already mentioned, the occupants move along the building's traversable cells and doorways, represented by the graph's nodes and edges. Our occupants' movement

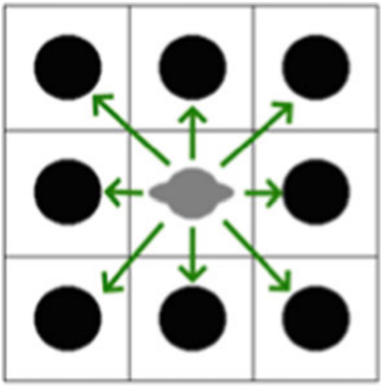


Fig. 4 Occupant's movement possibilities (Moore's neighbour)

model follows the cellular automata (CA) paradigm. In a more traditional CA model, each cell has the appropriate size to accommodate a single occupant, typically 40 cm × 40 cm, and the adjacent cells are a step away. Thus, an occupant on a node can pursue their way by moving to an adjacent node, as shown in Fig. 4.

The graph's nodes represent the elementary cells and the doorways in our building representation model. However, we do not need to decompose de building in 40 cm × 40 cm elementary cells, which allows a building to be represented by a significantly lower dimension graph, leading to computational advantages. So, instead of one occupant per node, as on a traditional CA model, the number of occupants is proportional to the cell area that corresponds to that node. As the graph's nodes positions are the coordinates of the cells and doorways' geometric centres, the occupant's distance to travel to the adjacent node is variable. It depends on the area of the cells and their position within it. Thus, the occupant's movement cannot be made from one node of the graph to the adjacent one as if it were a step away, and we have to model that movement between nodes.

A Two-Level CA Approach Model for Occupant's Movement Simulation

In order to explore the advantages provided by the model of representation of the building presented here, we created a new model for the occupant's movement simulation that considers a two-level CA approach consisting of two phases: macroscopic level phase and microscopic level phase. The occupant's movement between any two nodes is what we call macroscopic level movement, where the various occupants on a node may be seen as moving as a whole to the next node. However, we pretend to simulate each occupant's movement at a microscopic level, so we must consider that the occupants move over the graph's edges. Thus, the occupants' movement at the microscopic level refers to the occupants' movement on the graph nodes and edges or through the cells and doorways shown in Fig. 3.

Macroscopic level movement

The occupants move according to a strategy that considers the following two main aspects: (i) their familiarity with the building; (ii) the existence of emergency signs, as shown in the flowchart of Fig. 5.

Knowing the space, the occupant continues his way to the exit, following the shortest path. Therefore, we can use graph theory and adopt one of the algorithms commonly used to solve the problem of determining the shortest path, such as the Floyd–Warshall algorithm that we use in our experiments. Not knowing the space, the occupant adopts one of two strategies: (i) follows the emergency signs installed in the building; (ii) in the absence of signage, which is usual in residential buildings,

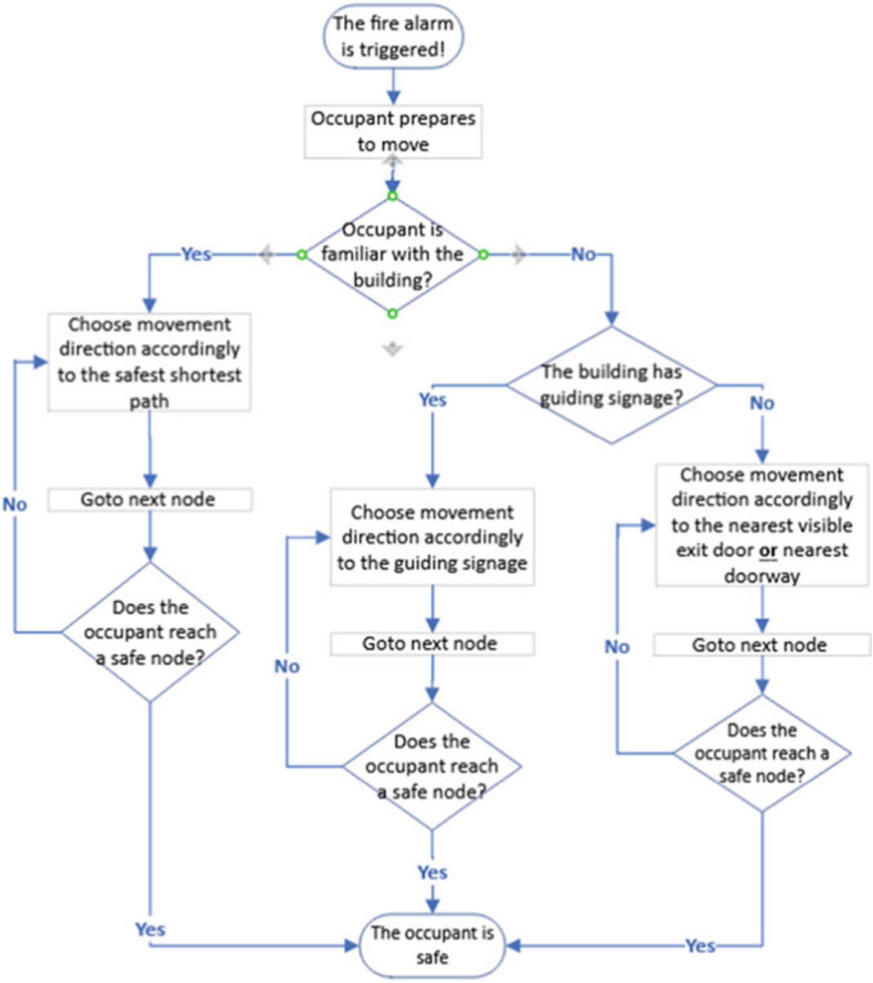

The fire alarm is triggered!
Occupant prepares to move
Occupant is familiar with the building?
Yes
No
Choose movement direction accordingly to the safest shortest path
Goto next node
Does the occupant reach a safe node?
No
Yes
The building has guiding signage?
Yes
No
Choose movement direction accordingly to the guiding signage
Goto next node
Does the occupant reach a safe node?
No
Yes
Choose movement direction accordingly to the nearest visible exit door or nearest doorway
Goto next node
Does the occupant reach a safe node?
No
Yes
The occupant is safe

Fig. 5 Occupant's strategy to exit the building

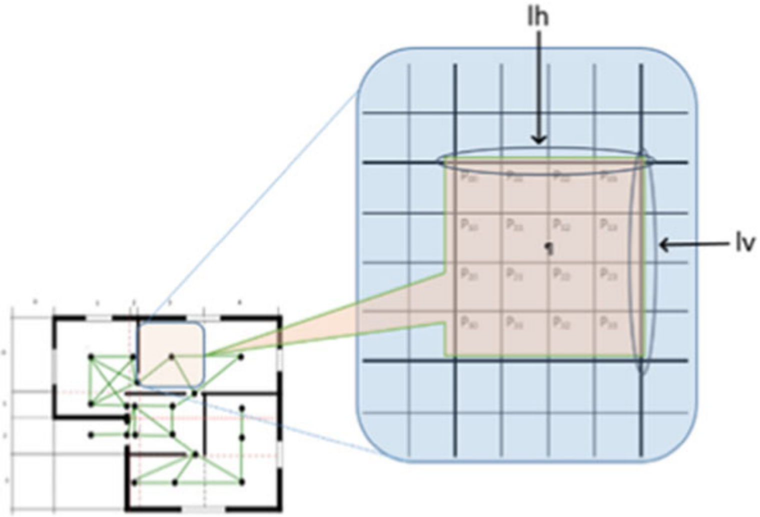


Fig. 6 Each cell is virtually divided into a grid to accommodate the occupant's movement

the occupant continues on his way, moving at each moment to the nearest doorway in his field of vision.

Based on the chosen strategy, an occupant positioned on a node of the graph moves to an adjacent node, according to a CA model. So, at phase one of our model, the occupant knows the next node to pursue in his strategy, establishing their movement direction. However, because the distance between nodes is more than a single step, the occupants move to their destination, according to the microscopic level movement phase model.

Microscopic level movement

Each elementary cell is virtually divided into a grid for modelling the occupant's movement at the microscopic level, as shown in Fig. 6. Each grid consists of $L * C$ squares of 40 * 40 cm^2, where: $L = \frac{lv}{0.4}$ e $C = \frac{lh}{0.4}$.

An occupant positioned at a square P_{ij} moves to an adjacent Moore neighbour square until he reaches a square P'_{ij}, leading him to the adjacent cell chosen at the macroscopic phase. Figure 7 defines which grid positions lead the occupant to move to the next adjacent cell.

Let G be a grid with $lh \times lv$ squares, and let P_{ij} be the notation for each grid square, where $0 \le i < lv$ and $0 \le j < lh$, and considering that, each square P_{ij} can be empty or occupied. At this phase of the movement process, the occupant O knows the adjacent node N_{ij} to pursue its way to exit the building. In Fig. 8, *UL* refers to the movement to the upper-left neighbour node. In Fig. 9, *VU* refers to the movement to the upper side neighbour node.

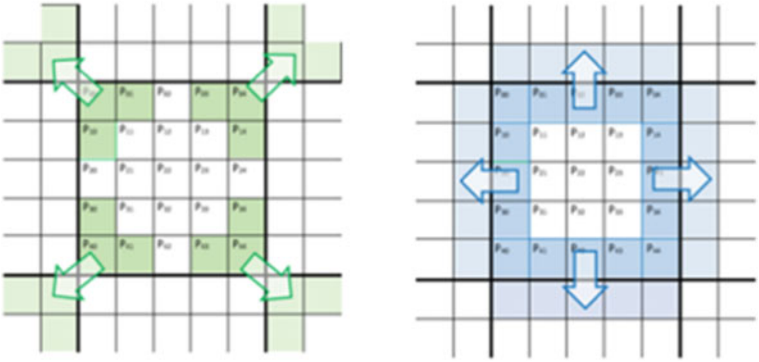


Fig. 7 Grid limit positions: when an occupant is moving to an adjacent diagonal node (left image); when an occupant is moving to an adjacent horizontal or vertical node (right image)

```
O IS IN NODE $N_{ij}$ POSITION $P_{ij}$
CASE DIRECTION = UL:
    WHILE O NOT IN [$P_{00}$ OR $P_{01}$ OR $P_{10}$]
        IF ($P_{i-1,j-1}$ = EMPTY) O MOVES TO $P_{i-1,j-1}$
        ELSE IF ($P_{i,j-1}$ = EMPTY) O MOVES TO $P_{i,j-1}$
        ELSE IF ($P_{i-1,j}$ = EMPTY) O MOVES TO $P_{i-1,j}$
        ELSE IF ($P_{i-1,j+1}$ = EMPTY) O MOVES TO $P_{i-1,j+1}$
        ELSE IF ($P_{i+1,j-1}$ = EMPTY) O MOVES TO $P_{i+1,j-1}$
        ELSE O STAY ON $P_{ij}$
    END WHILE
    REPEAT
        IF ([$P_{L-1,C-1}$ OR $P_{L-1,C-2}$ OR $P_{L-2,C-1}$] OF NODE $N_{i-1,j-1}$)=EMPTY
          O MOVES TO NODE $N_{i-1,j-1}$
        ELSE O STAY ON NODE $N_{ij}$
    UNTIL O IS IN NODE $N_{i-1,j-1}$
```

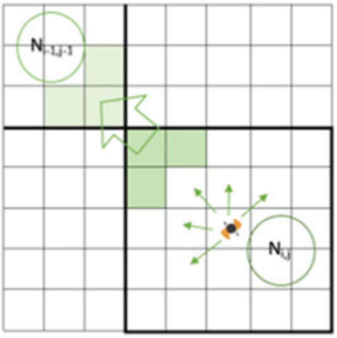


Fig. 8 Occupant's movement to the upper-left adjacent node: graphic representation and pseudocode

```
O IS IN NODE $N_{ij}$ POSITION $P_{ij}$
CASE DIRECTION = VU:
    WHILE O NOT IN [$P_{0,0..C-1}$]
        IF ($P_{i-1,j}$ = EMPTY) O MOVE TO $P_{i-1,j}$
        ELSE IF ($P_{i-1,j-1}$= EMPTY) O MOVE TO $P_{i-1,j-1}$
        ELSE IF ($P_{i+1,j+1}$ = EMPTY) O MOVE TO $P_{i+1,j+1}$
        ELSE IF ($P_{i,j-1}$ = EMPTY) O MOVE TO $P_{i,j-1}$
        ELSE IF ($P_{i,j+1}$ = EMPTY) O MOVE TO $P_{i,j+1}$
        ELSE O STAY ON $P_{ij}$
    END WHILE
    REPEAT
        IF ([$P_{L-1,0}$ OR ... OR $P_{L-1,C-1}$] OF NODE $N_{i-1,j}$)=EMPTY
          O MOVES TO NODE $N_{i-1,j}$
        ELSE O STAY ON NODE $N_{ij}$
    UNTIL O IS IN NODE $N_{i-1,j}$
```

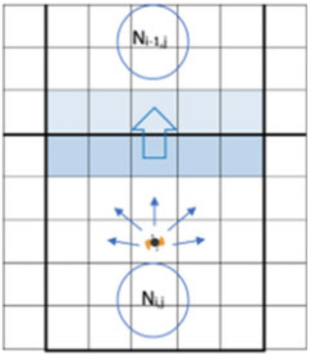


Fig. 9 Occupant's movement to the upper vertical node: graphic representation and pseudocode

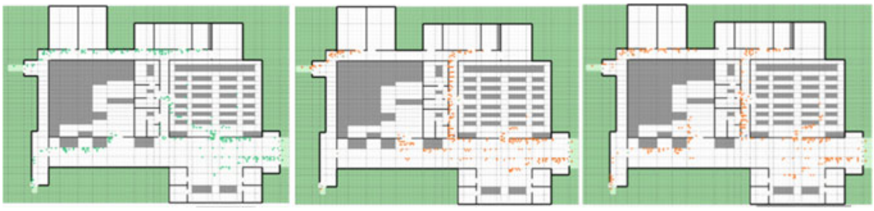


Fig. 10 Evacuation route patterns: if the occupants are familiar with the building (left); the occupants do not follow the guiding signage (middle); the occupants follow guiding signage (right)

4 Evaluating the Models: Simulator, Experiments and Results

To evaluate the models, we develop a Web simulator platform that allows characterising and representing a building by its floors according to the model previously described. One of the platform subsystems is a Web application for the building's physical and geometric representation, which allows the representation of the floors and all elements influencing the building's evacuation. The other subsystem is a multi-agent system for simulating the building evacuation, implementing the occupant's movement model herein presented. First, we represent the 2000 m^2 of the LNEC Congress Centre using the representation model presented in this paper. Second, we considered a hypothetical congress with 350 people in the space for the occupant's movement model testing. Then, we perform simulations for each of the following scenarios: (i) All occupants are familiar with the congress area and know how to exit the building safely; (ii) none of the occupants is familiar with the congress space, but with no emergency signalling, they will continue their way towards the exit, choosing at each moment to the nearest doorway; (iii) none of the occupants is familiar with the congress area, but they follow the emergency signage. Figure 10 shows the occupant's evacuation route pattern for the three scenarios under study and evaluation.

5 Discussion

The tests enabled the validation of the building representation and occupant's movement models. The proposed solution ensures the geometric and physical building representation, allowing its complete characterisation in terms of what is needed for analysing the fire conditions in a building, like the installed fire detectors, sensors, and emergency signs. The representation is done graphically for human visualisation and perception. It also provides all necessary data to be used by the multi-agent simulator system, which uses a graph representing the building. Agents represent fire detection devices, sensors, and emergency signs. Concerning the occupants' movement modelling, the two-level CA model herein proposed performs adequately, allowing to simulate the occupant's movement in their way to exit the building.

The experimental scenarios aim to simulate and evaluate our two-level CA movement model for each occupant's movement strategies presented in Fig. 5. If the occupants are familiar with the building, they follow the shortest route to the exit. On the other side, if they are unfamiliar with the building, two strategies are tested: the occupants pursue their way towards the nearest visible doorway or follow the building emergency guiding signage. Figure 10 presents the route evacuation patterns the occupants take on their way to leave the building. A similar behaviour pattern is observable between scenarios (ii) (none of the occupants knows the building) and (iii) (the occupants follow the guiding signage). The difference is that without guiding signage (Fig. 10), and accordingly with the adopted strategy, the occupants "choose" to follow his way walking to the visible exit doors (E2, E3 or E4), even if they are closer to the exit door E1, they do not "see".

6 Conclusion and Future Work

The simulation tests demonstrate the platform's viability for the geometric and physical building representation and the occupant's movement modelling. The main contributions of this paper refer to the novelty of the approaches regarding building representation and the new two-level CA approach models. The model building representation allows the building's geometric and physical representation and fire safety devices. Furthermore, it allows the representation of a building by a much lesser dimension graph, which directly impacts computing processing time. On the other hand, the new two-level CA approach model for occupant's movement simulation proposed here benefits from the advantages offered by the model building representation, allowing for more fastest and reliable simulations. We plan to provide tools to integrate geometric data from CAD applications and fire model propagation in future work. We also plan to integrate the multi-agent recommender system to guide the occupants to a safe place [1] to test and evaluate the above-referred paradigm shift that we are studying on our ongoing Ph.D. thesis.

References

1. Neto J, Morais AJ, Gonçalves R, Leça Coelho A (2019) A multi-agent system for recommending fire evacuation routes in buildings, based on context and IoT. Commun Comput Inf Sci:343–347
2. Ribeiro J, Almeida JE, Rossetti RJF, Coelho A, Coelho AL (2012) Towards a serious games evacuation simulator. In: TroitzschKG, Moehring M, Lotzmann U (eds) ECMS 2012 proceedings
3. Coelho AL, Neto J (2020) A importância da modelação das condições de segurança ao incêndio na reabilitação de edifício. In: Livro de Atas do ENCORE 2020 - 4° Encontro de Conservação e Reabilitação de Edifícios, pp 345–356

4. Gwynne S, Galea ER, Owen M, Lawrence PJ, Filippidis L (1999) A review of the methodologies used in the computer simulation of evacuation from the built environment. Build Environ 34(6):741–749
5. Hamacher HW, Tjandra SA (2001) Mathematical modelling of evacuation problems: a state of art
6. Schadschneider A, Klüpfel H, Kretz T, Rogsch C, Seyfried A (2011) Fundamentals of pedestrian and evacuation dynamics. In: Multi-agent systems for traffic and transportation engineering. IGI Global, Hershey
7. Dhamala TN (2014) A survey on models and algorithms for discrete evacuation planning network problems. J Ind Manag Optim 11(1):265–289
8. Kobes M, Helsloot I, de Vries B, Post JG (2010) Building safety and human behaviour in fire: a literature review. Fire Saf J 45(1):1–11
9. Ronchi E, Nilsson D (2013) Fire evacuation in high-rise buildings: a review of human behaviour and modelling research. Fire Sci. Rev. 2(1):7
10. Leça Coelho A, Neto J (2019) Modelo de Análise das Condições de Segurança ao Incêndio em Edifícios Existentes (MACSI_2E), Lisboa

Safety State Assessment of Network Control System Based on Belief Rule Base

Ying Han, Limin Xiao, Jie Luo, Jie Zeng, and Xin Su

Abstract The current network control system (NCS) cannot assess the system safety state in a timely, comprehensive, and accurate manner, which leads to serious security problems in NCS. Directing at the defects of existing security state assessment models for the NCS, a method of safety state assessment of the NCS based on the belief rule base (BRB) expert system is proposed in this paper. Firstly, the expert system of the BRB is used to combine qualitative knowledge with quantitative monitoring data. Then, the evidential reasoning (ER) algorithm is used for knowledge reasoning, and the initial parameters of BRB model are optimized. Finally, taking the data of a gas NCS as an example, the experimental results illustrate that the assessment accuracy is higher than that of back propagation (BP) and support vector machines (SVM) evaluation models.

Keywords Belief rule base · ER reasoning · Safety state assessment · Expert system

1 Introduction

In recent years, the safety state assessment of the network control system (NCS) has gradually become a research focus, and the safety state assessment of the NCS is an important research method to obtain accurate safety status of the NCS. Effective safety state assessment gives expression to the health situation of the system environment. It can detect system vulnerabilities and external malicious attacks in advance

Y. Han (✉)
School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
e-mail: S190131017@stu.cqupt.edu.cn

L. Xiao · J. Zeng · X. Su
Department of Electronic Engineering, Tsinghua University, Beijing, China

J. Luo
China Academy of Telecommunications Technology, Beijing, China

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_68

and provide a solid theoretical guarantee for the administrator to make decisions to reduce business losses and ensure the stable operation of NCS.

1.1 The Safety State Assessment Methods

Safety state assessment is widely applied in safety monitoring of complex systems, in which observation information is used to evaluate system safety state. At present, there are two research methods of safety state assessment, one is the statistical model-based safety state assessment method, and the other is the data-driven health assessment method.

The statistical model-based safety state assessment methods. The statistical model-based safety state assessment methods include various statistical models and filters, such as the Kalman filters, the particle filters, and the key performance indicator methods. These methods can be applied to analyze and evaluate in light of network noise and characteristics. Whereas, the methods are difficult to establish accurate and reasonable models for complex control systems.

The data-driven health assessment methods. The data-driven health assessment methods include three sub-methods: the qualitative knowledge-based safety assessment method, the quantitative information-based safety assessment method, and the semi-quantitative (quantitative information and qualitative knowledge)-based safety assessment method. The quantitative information-based safety assessment methods include Petri net model and expert system. These methods make predictions based on known qualitative knowledge. Considering that the control system is complicated and contains a great deal of uncertain information, it is difficult to apply to a single qualitative knowledge to construct an accurate evaluation model. Although a large number of indicators used in the evaluation process can improve the accuracy of the evaluation, it also increases the computational complexity, thereby affecting the computational efficiency. The quantitative information-based health assessment methods include support vector machines (SVM) model and artificial neural network model. These methods train model parameters based on the quantitative data of the system. Due to prior expert experience and limited training samples, it is inaccurate that the quantitative information models obtain evaluation results only based on small-scale samples. The semi-quantitative-based safety assessment methods include dynamic Bayesian network models, hidden Markov models, and fuzzy neural network models. These methods combine qualitative knowledge and quantitative methods. Firstly, the expert experience is used to set initial parameters. Next, the initial parameters are optimized according to the observed data. Finally, the small-scale samples are used to obtain better evaluation results.

In summary, the evaluation model based on semi-quantitative information has advantages in assessing the safety state of the NCS. Nevertheless, these methods also have some disadvantages. Dynamic Bayesian networks and hidden Markov models show superior performance only when dealing with uncertain information, and they cannot solve uncertain and fuzzy information. The fuzzy neural network can resolve the uncertain and fuzzy information well, but it cannot work out the probability uncertainty information. To assess the safety state of the control system more accurately, an expert system based on the BRB is proposed to assess the safety state of the NCS.

2 Related Work

The BRB is proposed according to D-S evidence reasoning, IF-THEN rule expert system, and ER algorithm. It has a good modeling ability for nonlinear characteristic data with fuzzy uncertainty or probabilistic uncertainty. BRB has now performed outstandingly in fault diagnosis and prediction. Liu et al. [1] propose an alternative ensemble learning method for BRB classification systems, and they confirm the accurateness of the proposed approach on systematization problems. Hu et al. [2] propose a distributed BRB model reasoning method, which improves the algorithm efficiency by dividing the algorithm model into many BRB sub-models. To make the prediction of network safety state better utilizing quantitative data and expert knowledge, a predictive model known as cloud belief rule base (CBRB) model is introduced [3]. The CBRB model describes the key point of belief rule by utilizing the cloud model, which is clearer to describe expert knowledge. New optimization models for training a BRB are proposed in Yang et al. [4]. The new model is for locally training optimization problems. Zhou et al. [5] developed a BRB prediction model and put it in using the fault diagnosis technology. Fu et al. [6] utilize the decision tree classification method to analyze data rules and form related rules, and then a new rule representation method based on reference interval is introduced, which can construct rule base in light of the belief degree of related data. To improve the accuracy of the safety model, a safety evaluation method [7] based on BRB with attribute accuracy with combining belief rule accuracy is proposed. Therefore, it has the potential to apply the BRB model to the safety state assessment of the NCS and to confirm the model regarding a specific control system.

3 The Safety State Assessment Model of NCS

To assess the health status of the control system accurately, the BRB expert system must be used first to fuse the health status of the important characteristic attributes in the system. Then, combine the quantitative monitoring data and qualitative knowledge in the control system. Finally, use the FMINCON function in MATLAB to optimize the parameters of the expert system and evaluate the health status of the control system accurately. The model intends to solve the problems of difficulty in establishing the control system safety state assessment model, insufficient effective data acquisition, and low accuracy of expert system evaluation.

3.1 BRB-Based Model of Safety State Assessment

In the proposed BRB evaluation model, the regularization process is not simply composed of a series of belief rules but introduces the premise of attribute weights and rule weights. Meanwhile, the model has a good ability to deal with random and fuzzy uncertain information. The description of the *k*th rule based on the BRB model is calculated by

$$\begin{aligned}&R_k : \text{If}\, x_1 \text{ is } A_1^k \Lambda x_2 \text{ is } A_2^k \Lambda \ldots \Lambda x_M \,\text{is}\, A_M^k\\&\text{Then}\, \{(Q_1, \beta_{1,k}),\ (Q_2, \beta_{2,k}), \ldots, (\mathrm{Q}_N, \beta_{N,k})\}\\&\text{With a rule weight}\theta_k\text{and attribute weight } \delta_{1,k}, \delta_{2,k}, \ldots, \delta_{M,k}\end{aligned} \tag{1}$$

Among them, R_k is the *k*th rule of the BRB assessment model. $A_i^k(i = 1, 2, \ldots M_k)$ represents the reference value of the *i*th input premise attribute in the *k*th rule; D_k represents the result set. The reference value of the safety state of the control system is set to "high," "medium," and "low," expressed as $Q = (Q_1, Q_2, Q_3) = (G, S, P)$, where *G* means good health, *S* means sub-health, and *P* means poor health. $\beta_{j,k}(j = 1, 2, \ldots, N)$ means the belief of the *j*th evaluation result Q_j in the *k*th rule relative to the output part, and *N* represents the sum of the belief degree. $\theta_k(k = 1, 2, \ldots, L)$ denotes the rule weight of the *k*th rule, $\delta_{1,k}(i = 1, 2, \ldots, M)$ represents the weight of the *i*th premise attribute in the *k*th rule, the initial values are assumed to be $\delta_{1,k} = 1$.

3.2 Inference of the Safety State Assessment Model

To obtain the overall safety state of multiple index attributes of the NCS, the ER algorithm is introduced to integrate the safety factors of the NCS. The assessment result of the safety state can be expressed as four steps.

(1) Solve and express the premise belief degree of the NCS.

The belief of the *l*th attribute x_l relative to the reference value is calculated by

$$\varpi_j^l = \begin{cases} \frac{C_{l(k+1)} - x_l^*}{C_{l(k+1)} - C_{lk}}, & j = k \quad \text{if}\, C_{lk} \le x_l^* \le C_{l(k+1)} \\ \frac{x_l^* - C_{lk}}{C_{l(k+1)} - A_{lk}}, & j = k + 1 \\ 0, \quad j = 1, 2, \ldots |x_l|, & j \ne k, k + 1 \end{cases} \tag{2}$$

where ϖ_j^l represents the matching degree of the *j*th rule at the time *l*. C_{lk} is the reference point of the *l*th network characteristic in the *k*th rule. x_l^* means the input of the missing data compensation model. $|x_l|$ represents the number of rules composed of feature data at the time *l*.

Next, the matching degree between input network characteristics and the belief rules is described as following

$$\overline{v}_i = \frac{v_i}{\max\limits_{i=1,\ldots,M}\{v_i\}}, \quad 0 \le \overline{v}_i \le 1$$
$$\varpi_k = \prod_{i=1}^{M}\left(\varpi_k^i\right)^{\overline{v}_i} \tag{3, 4}$$

$\overline{v}_i$ is the relative weight of the historical data at the time i.
ϖ_k is the matching degree of input characteristics to rule k.
M represents the number of input features in rule k.

(2) Calculate the activation weight of belief rules for control systems.

When the measured control system characteristic attributes are input as input attributes, the activation weights of each input attribute to k rules are different, which are calculated by

$$\psi_k = \frac{\vartheta_k \varpi_k}{\sum_{l=1}^{L} \vartheta_l \varpi_l}, \quad k = 1, \ldots L_H \tag{5}$$

where ψ_k means the activation weight of the kth belief rule, and ϑ_k is the weight of the kth belief rule.

(3) Calculate the belief degree of output results for the control system.

The belief relative to the evaluation result Q_j can be obtained by calculating the belief ς_f of the control system output and combining the L_H rules of the control system. Calculated by ER analytic algorithm, the calculation method is given by

$$\varsigma_f = \frac{\mu\left[\prod_{k=1}^{L_H}\left(\psi_k \zeta_{f,k} + 1 - \psi_k \sum_{j=1}^{F} s_{j,k}\right) - \prod_{k=1}^{L_H}(1 - \psi_k \sum_{j=1}^{F} s_{j,k})\right]}{1 - \xi\left[\prod_{k=1}^{L_H}(1 - \psi_k)\right]}$$
$$\xi = \left[\sum_{f=1}^{F}\prod_{k=1}^{L_H}\left(\psi_k \varsigma_{f,k} + 1 - \psi_k \sum_{j=1}^{F} \varsigma_{j,k}\right) - (F - 1)\right.$$
$$\left. \times \prod_{k=1}^{L_H}(1 - \psi_k \sum_{j-1}^{F} \varsigma_{j,k})\right]^{-1} \tag{6}$$

ς_f means the ultimate belief degree for the fth safety state level.
L_H is the number of belief rules in the health assessment model.
(4) The ultimate output of the BRB system is to combine all the rules in the BRB, that is, to combine the safety state of the ith feature of the control system at time t.
The ultimate assessed state of health can then be described by

$$y = H(t) = \sum_{f=1}^{F} u\big(H_f\big)\varsigma_f \tag{7}$$

Through the above four steps, $H(t)$ can be obtained by the final fth safety state level H_f expected utility $u\big(H_f\big)$, which reflects the safety state of the control system.

3.3 Parameter Optimization Model of BRB

The expected utility y of the control system is calculated by (7), which reflects the safety state of the NCS. To make the BRB output y as close to the observed value as possible, it is essential to train the parameters of the input premise weight v_i, the output belief degree $\varsigma_{j,k}$, the rule weight ϑ_k, and the utility $u\big(H_f\big)$ of the evaluation result H_f (or Q_j) in the BRB. Since the training parameters are numerical, the following optimization objectives can be calculated by

$$\min_{V}\{\xi(V)\}$$
$$\text{s.t.equation}(1) - (7)$$

where $V = \big[\vartheta_K, v_i, \varsigma_{j,k}, u\big(H_f\big)\big]^{\mathrm{T}}$ is a column vector consisted of the BRB system parameters.

$\xi(V) = \frac{1}{T}\sum\limits_{m=1}^{T}\big(y_m - \widehat{y_m}\big)^{\mathrm{T}}$ represents the mean square error objective function.

4 Case Analysis

The effectiveness and reliability of the proposed ER-BRB model are verified by an example of a gas control system. Firstly, the system sensors collect real health event data in the gas control system, and the system monitoring indicators include pressure, temperature, and traffic. The traffic of the gas control system is closely related to urban gas consumption, so the pressure and temperature of the gas control system are selected as the premise attributes. Due to the complex parameters of each component of the gas control system, the safety state reference value of the gas control system is Simplified as high health coefficient, medium health coefficient and low health coefficient denoted as high, medium, and low.

Expert knowledge plays an important role in small sample classification. In the BRB model, the setting of the rules is important as well as the setting of temperature and pressure indicators. The premise attribute weight $\delta_{i,k}$ and the rule weight θ_k are set to 1. When setting the temperature and pressure reference values of the gas control system, the number of rules depend on the number of safety state reference values.

Table 1 Semantic reference values of each index

State	Reference point	Reference value
Temperature	NT, MT, HT	1,2,3
Pressure	NP, MP, HP	1,2,3
State of safety	*G*, *S*, *P*	

The degree of model calculation will also become more complicated as the number of rules increases.

In light of expert knowledge, there are three reference levels for setting the temperature attributes of the gas system, including normal, high, and high, represented by NT, MT, and HT. Furthermore, there are three reference levels for setting the pressure properties of the gas system, including normal, (medium) high, and high, expressed as NP, MP, and HP. The safety state reference level of the gas control system based on the BRB model is set as "high," "medium," and "low," expressed as G, S, and P. The quantitative results of the three indicators are shown in Table 1.

The pressure and temperature reference values of the gas control system include three levels, a total of nine belief rules. Based on expert knowledge, the health state assessment model of the gas control system based on the BRB is established. The k rule can be calculated by

$$\begin{aligned} & R_k : \text{Iftemperatureis } A_1^k \Lambda \text{pressure} is A_2^k \\ & \text{Thensafetystateis} \{(1, \beta_{1,k}), (2, \beta_{2,k}), \ldots, (3, \beta_{N,k})\} \\ & \left(\sum_{i=1}^{M} \beta_{N,k} \le 1 \right) k \in \{1, 2, \ldots, 9\} \end{aligned} \tag{8}$$

Based on expert knowledge, the initial parameters of the BRB model are shown in Table 2. In Table 2, when the temperature is high and the pressure is high, the health coefficient of the gas control system is very low. In the first rule NT&&NP, it

Table 2 Gas control system state rule table

No	Temperature && pressure	Output distribution
1	NT&&NP	$\{(Q_1, 0.9), (Q_2, 0.1), (Q_3, 0)\}$
2	NT&&MP	$\{(Q_1, 0), (Q_2, 0.8), (Q_3, 0.2)\}$
3	NT&&HP	$\{(\mathrm{Q}_1, 0.1), (Q_2, 0.1), (Q_3, 0.8)\}$
4	MT&&NP	$\{(Q_1, 0.3), (Q_2, 0.7), (Q_3, 0)\}$
5	MT&&MP	$\{(\mathrm{Q}_1, 0), (Q_2, 1), (Q_3, 0)\}$
6	MT&&HP	$\{(Q_1, 0), (Q_2, 0.1), (Q_3, 0.9)\}$
7	HT&&NP	$\{(Q_1, 0), (Q_2, 0.2), (Q_3, 0.8)\}$
8	HT&&MP	$\{(\mathrm{Q}_1, 0), (Q_2, 0.1), (Q_3, 0.9)\}$
9	HT&&HP	$\{(\mathrm{Q}_1, 0), (Q_2, 0), (Q_3, 1)\}$

indicates that the pressure and temperature of the gas system are within the normal range, and the healthy state of the gas control system can be regarded as a state with high health coefficient. Therefore, the safety state of the gas control system is assigned as $\{(Q_1, 0.9), (Q_2, 0.1), (Q_3, 0)\}$. The fifth rule MT&&MP explains that the safety state of the gas control system changes from the state of high coefficient to the state of medium coefficient, and the pressure and temperature of the gas system are in the medium state. Therefore, the state reflecting the gas control system is assigned as $\{(Q_1, 0), (Q_2, 1), (Q_3, 0)\}$. The results of the health status distribution of the gas control system generated by the initial BRB model are listed in Table 2.

The results of the gas control system created by the initial BRB model is shown in Fig. 1. It can be known from Fig. 1 that the expert value cannot well reflect the safety state of the monitored gas control system, so the FMINCON function in MATLAB is applied to optimize the parameters of the gas control system, as shown in Fig. 2. The optimized BRB model can evaluate the safety state of the gas control system more accurately.

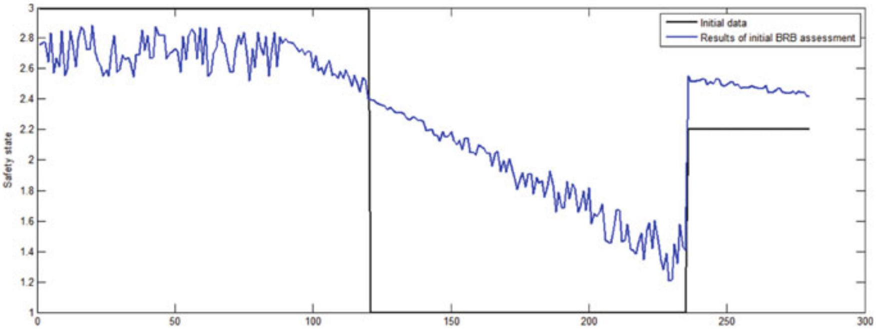


Fig. 1 Results of initial BRB assessment

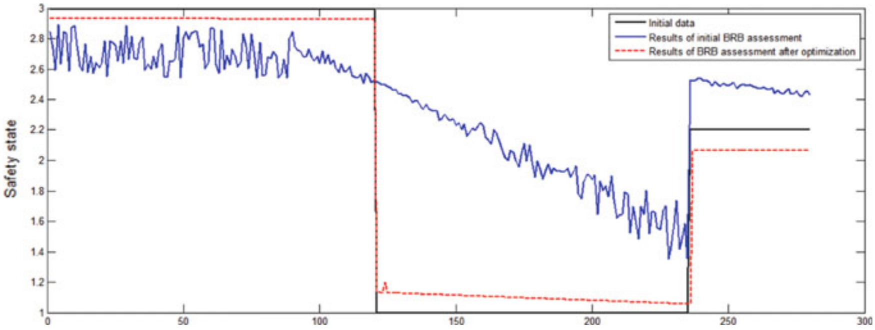


Fig. 2 Results of BRB assessment after optimization

5 Comparison of Simulation Results

In this section, we provide theoretical calculation and simulation results to prove the results mentioned above. To prove the accuracy and reliability of the evaluation method, two prediction and evaluation models, BP neural network model and the SVM model, are selected for comparison. The BP neural network model is a typical semi-quantitative model, whose output can reflect the change of the monitoring data in the gas system and the fitting degree is high under the condition of high health coefficient. However, as shown in Fig. 3a, the fitting degree is low under the condition of low neutralization of health coefficient. An SVM model is one of the models based on quantitative information. Compared with other neural network models, it has higher performance, but as demonstrated in Fig. 3b, the fitting degree of SVM is not good, resulting in inaccurate safety assessment of the gas control system. Compared with these two models, the BRB evaluation model is more accurate.

In Table 3, we can see that the optimized the BRB model can accurately evaluate the state of the gas control system, and its mean square error value is less than that of

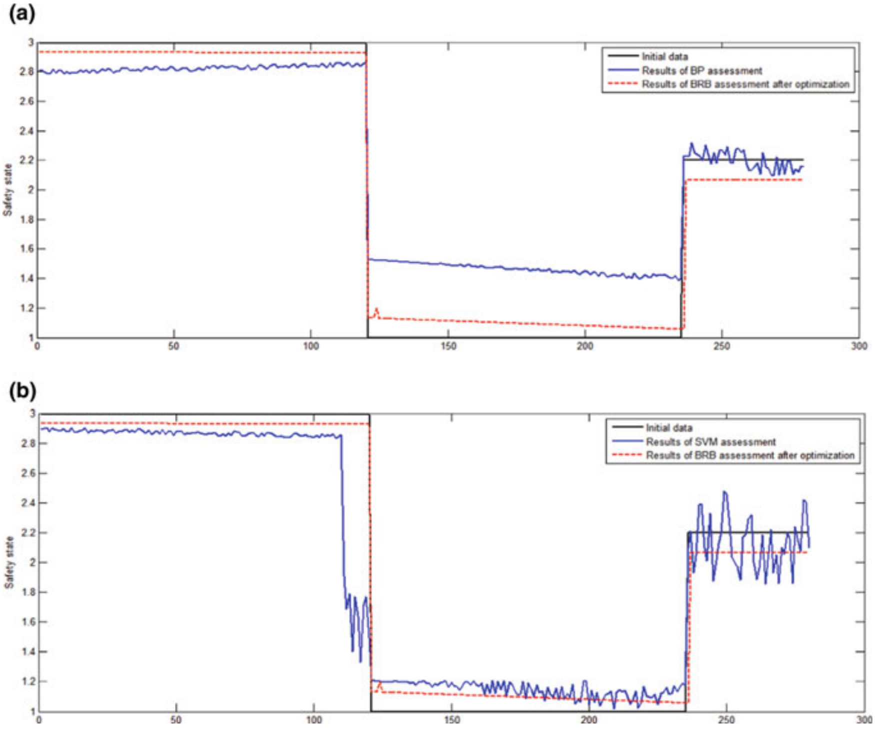


Fig. 3 Comparative study assessment results. **a** Results of BP assessment. **b** Results of SVM assessment

Table 3 MSE comparison results

Model	MSE
Initial BRB	1.857
Optimized BRB	0.151
SVM	0.912
BP neural network	1.336

the SVM and BP neural network model, and the error interval is limited in a narrow range.

6 Conclusion

The safety state evaluation method of the control system based on the BRB is proposed. Expert knowledge and quantitative monitoring data were applied to find the safety state evaluation model of BRB. To enhance the validity of the evaluation model, ER algorithm was introduced for knowledge reasoning, and the initial parameters of the established BRB model were optimized to enhance the evaluation accuracy.

The case based on the state assessment of the gas control system has shown that the proposed model can well evaluate the operation state of the gas control system with high applicability to practical engineering problems. When an accurate mathematical model cannot be established and a great deal of control system failure data cannot be obtained, the model can use expert knowledge to evaluate the safety state of industrial control systems.

To confirm the effectiveness of the model, the model in this paper is compared with the. The comparisons with BP neural network and SVM model show that the model has obvious advantages when expert knowledge can be obtained and the monitoring data is limited. This work will provide a reference for future safety state assessments.

Acknowledgements This work was supported by National Key R&D Program of China (2020YFB1806702) and DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD Funded Project (20202000659).

References

1. Liu W, Wu W, Wang Y (2019) Selective ensemble learning method for belief-rule-base classification system based on PAES. Big Data Min Analyt 2(4):306–318
2. Hu Q, Li C, Lu Y (2020) A novel construction and inference methodology of belief rule base. IEEE Access 8:209738–209749
3. Hu G, Qiao P (2016) Cloud belief rule base model for network security situation prediction. IEEE Commun Lett 20(5):914–917

4. Yang J, Liu J, Xu D (2007) Optimization models for training belief-rule-based systems. IEEE Trans Syst Man Cybernet Part A Syst Hum 37(4):569–585
5. Zhou Z, Chang L (2016) A new BRB-ER-based model for assessing the lives of products using both failure data and expert knowledge. IEEE Trans Syst Man Cybernet Syst 46(11):1529–1543
6. Fu Y, Yin Z, Su M et al (2020) Construction and reasoning approach of belief rule-base for classification base on decision tree. IEEE Access 8:138046–138057
7. Feng Z, He W, Zhou Z et al (2021) A new safety assessment method based on belief rule base with attribute reliability. IEEE/CAA J Automat Sin 8(11):1774–1785

Bringing Explainability to Model Deployment Pipeline in Deep Learning Workbench

Alexander Demidovskij, Tatiana Savina, Alexander Suvorov, Mikhail Fedorov, and Yury Gorbachev

Abstract Widespread use of highly accurate and trustworthy deep learning architectures is becoming a noticeable trend in the industry. Model accuracy and inferencing performance traditionally remain the two important factors to be considered before model deployment to any business application. Additionally to these two requirements, the problem of model explainability is becoming increasingly acute. In this paper, we propose a methodology for ensuring that pretrained deep learning models provide optimal performance, have an acceptable accuracy level, and make trustworthy decisions. The methodology is tested on a classification computer vision model, taking into account specified business requirements.

Keywords Deep learning · Explainable AI · Inference · OpenVINO

1 Introduction

Recent advances in deep learning have significantly contributed to the rapid development of hardware and software capabilities and allowed to achieve superhuman performance of neural models across a variety of tasks. The exceptional performance

A. Demidovskij (✉)
Higher School of Economics, 25/12 Bolshaya Pecherskaya st., 603155 Nizhny Novgorod, Russia
e-mail: alexander.demidovskij@intel.com
URL: https://www.hse.ru/staff/demidovs

A. Demidovskij · T. Savina · A. Suvorov · M. Fedorov · Y. Gorbachev
Intel Corporation, 30 Turgeneva st., 603024 Nizhny Novgorod, Russia
e-mail: tatiana.savina@intel.com

A. Suvorov
e-mail: alexander.suvorov@intel.com

M. Fedorov
e-mail: mikhail.fedorov@intel.com

Y. Gorbachev
e-mail: yury.gorbachev@intel.com

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_69

has resulted in the extensive usage of such models in the industry. To get the model into production, several critical aspects must be considered, including its accuracy and inferencing performance, as well as the model's trustworthiness. Understanding the deep learning model's decision-making process is a quite complex task that puts emphasis on the issue of trust.

A set of techniques called explainable artificial intelligence (xAI) is currently being created specifically for understanding the rationale behind neural model decisions. To ensure that the deployment of neural models is beneficial to society, different ethical principles and regulatory frameworks for AI have been developed at the level of international organizations, governments, and private institutions. The General Data Protection Regulation (GDPR) [10] issued in the European Union in 2018 is one of the most important acts in the AI regulation domain. GDPR highlights the importance of providing meaningful information about the logic behind AI algorithm and its anticipated consequences, establishing the right to obtain human intervention to contest the decision. Similar principles of the explainability are expressed in the following documents: the Principles on Artificial Intelligence [9], the Directive on Automated Decision Making (Canada) [27], Ethical Norms for New Generation Artificial Intelligence (China) [28], US National Artificial Intelligence Initiative Act [29], and the Code of Ethics in the field of AI (Russia) [26]. Various decisions in the field of xAI are introduced by large companies, such as Google [12], Amazon [2], and Microsoft [15].

The growing attention from the international community demonstrates the crucial aspect of the usage of explainable AI methods for creating interpretable explanations from an ethical point of view. Along with interpretability, it is often required to accelerate neural models inferencing performance for the deploying hardware capabilities. These two important factors of model implementation constitute the main topic of this paper. We consider only a computer vision task, in particular image classification, and demonstrate a methodology that can be utilized to accelerate a model, applying a xAI technique to ensure its trustworthiness.

The structure of this work is as follows. Section 2 gives a brief overview of existing xAI methods. Section 3 describes the proposed methodology of preparing the model for production, which includes the integration of explanation methods as a verification step to ensure the quality of neural model predictions. A detailed evaluation of the methodology is provided in Sect. 4. The final section outlines the study results and directions for further research.

2 Background Study

There is a variety of explainable AI techniques designed to tackle the problem of reliability and transparency of neural models. They can be classified into the methods for analyzing and interpreting decision-making during the training process and post-training explanation techniques. Although the former is not the subject of this article, their enumeration and detailed descriptions can be found in [13]. We primarily focus on the post-training methods since it is often prohibitively expensive to introduce changes into the training process or pointless to retrain a model. We give brief descriptions of xAI methods that utilize a saliency map indicating the relative value of each pixel to the model prediction.

One of the well-known methods for evaluating trained black boxes models is Local Interpretable Model-agnostic Explanation (LIME) [23]. While LIME is relatively easy to comprehend, one of its constraints is the dissimilar behavior in various regions of the decision boundary due to the random sampling approach used to produce the explanations [1]. Another widely used technique is Shapley Additive explanations (SHAP) [14] method based on Shapley values. A significant drawback of SHAP is the computational time required to assess the model. Additionally, both LIME and SHAP were also shown to be vulnerable to adversarial attacks, resulting in the generation of misleading interpretations [25]. Further, we also should consider popular Class Activation Mapping (CAM) methods. White-box model-agnostic GradCAM method [24] utilizes the class-specific gradient information score flowing into the final convolutional layer to provide visual explanations. The main disadvantage of GradCAM is its inability to identify numerous occurrences of an object in an image.

The RISE [22] algorithm obscures an image to observe the effect on the model prediction for a specific class. The image is randomly masked by preserving a subset of the pixels, reducing pixel intensities to zero, and calculating the masked image confidence score. The procedure is applied to a set of randomly generated masks that have values between 0 and 1. The saliency map is calculated as a weighted sum of the random masks, with the weights representing the confidence score of the masked images. RISE algorithm is distinguished by its simplicity and model-agnostic characteristics, but also because it outperforms LIME and GradCAM in certain tasks [22]. Since RISE appears to be effective for interpreting classification models, we include it as part of the proposed methodology for analyzing a neural model.

3 Proposed Model Deployment Methodology

The preparation of a neural model for integration to a business application is a critical step in the deployment process. It is essential to adhere to a formal methodology that results in acquiring a model that fully satisfies business requirements. Following that, we analyze each step of the proposed methodology in details:

1. *Model selection* The first step in solving a business task is selecting a suitable neural model. Usually, during the deployment stage, the model architecture is already specified, and the model is trained or fine-tuned for a particular task. On the other hand, it is still quite common to encounter situations when it is necessary to find and fine-tune a model for specific use case. For example, in the OpenVINO ecosystem, Open Model Zoo [19] significantly facilitates the process of finding a

model by providing a selection of high-quality pretrained deep learning models with necessary information about them.

2. *Runtime environment selection* The increasing strictness of business requirements necessitates a highly efficient model runtime on the target accelerator. Additionally, due to the variety of use cases and accelerators, it is essential to provide a comprehensive and unified application programming interface (API). It is also important to note that both high-performance computing platforms and low-power edge devices are utilized in business applications. Several frameworks, such as OpenVINO [21], TensorRT [17], TVM [4] are designed to facilitate the unification of interfaces and assist in meeting the business requirements. The selection of the framework usually depends on the framework's compatibility with the specific target, the size of the runtime environment, the ecosystem's richness, and other factors.
3. *Evaluation of model performance characteristics* Inferencing performance is the essential criterion for measuring the quality of a neural model. Depending on the business requirements, there are two methods for assessing the model's inferencing performance: either minimizing latency or maximizing throughput (in computer vision, throughput is the number of images processed in a given amount of time). Typically, accuracy performance is the primary criteria for evaluating the model's quality during the training process. However, since the deployment and training environments are generally different, it can lead to changes in accuracy performance caused by peculiar properties of the environment. Thus, it is critical to assess the accuracy performance of a pretrained model in the deployment environment. Since this is a complex process involving multiple model executions on a dataset, it is convenient to use a tool that can assist in evaluating accuracy performance. In the OpenVINO environment, deep learning accuracy validation framework (Accuracy Checker) [18] is used to evaluate the accuracy of neural models, as well as to compare the accuracy of the model before and after the conversion to the intermediate representation format (IR—internal OpenVINO model format).
4. *Evaluation of model trustworthiness* After analyzing inferencing and accuracy performance, at this step, we recommend evaluating model trustworthiness by applying the xAI method to comprehend the decision-making process and get an assessment of the model from different perspectives. If all the requirements are met, we proceed to Step 8. If the accuracy or trustworthiness requirements are not satisfied, we need to return to Step 1 and either retrain the model or choose another one. If only the inferencing performance criterion is not met, we proceed to Step 5 to improve inferencing performance.
5. *Model optimization* An optimization technique that improves model performance while reducing model footprint is commonly needed to meet business requirements. Optimization methods can be divided into methods that require access to the model training or re-training process: weight pruning, filter pruning [3], and methods that do not require model training, such as shape reduction [5] and 8-bit quantization [8]. Quantization is a common way to accelerate neural model performance and reduce the footprint by lowering the precision of the model, for

example, from 32-bit floating-point number to 8-bit integer. Quantization should be selected depending on the accelerator since some edge accelerators do not support certain formats. For example, 16-bit floating-point quantization is recommended for Intel® Movidius™Neural Compute Stick 2 since it does not support 8-bit integer quantization. Section 4 demonstrates a significant acceleration of the model, using 8-bit optimization on a target that supports 8-bit inference. OpenVINO includes the post-training optimization tool [20] used to optimize pretrained neural models.

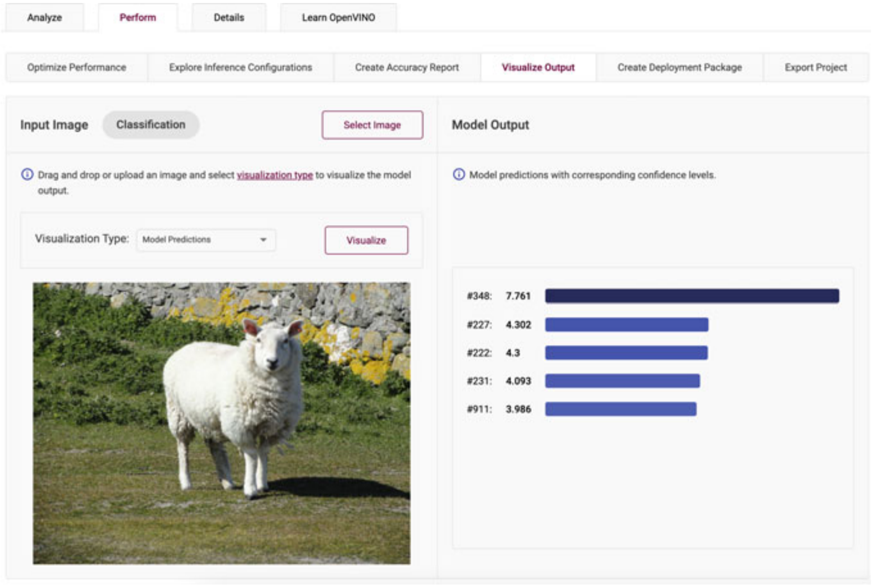
6. *Post-optimization performance characteristics assessment* While modern optimization techniques allow to obtain an accelerated version of the model, the majority of them are lossy and require model evaluation after the optimization. If the optimized model does not meet the business requirements, we recommend returning to Step 5 and either modifying the optimization method, or applying other optimization methods and re-evaluating the optimized model inferencing and accuracy performance. For example, the post-training optimization tool provides accuracy-aware optimization mode that enables to control the difference between the optimized and original model accuracy performance within a specified threshold.
7. *Evaluation of model trustworthiness after optimization* Even if the optimized model demonstrates high accuracy in the deployment environment, this does not guarantee that the model's decision-making process remains unchanged. As a result, it is necessary to re-evaluate the model's trustworthiness. For that, we recommend applying a xAI method to the optimized model for comparing its decision-making process to the original model's results obtained in the Step 4. If no degradation occurs, we proceed to Step 8. If there is a significant discrepancy, we need to return to Step 5 and change or adjust the optimization method.
8. *Integrating the model into the business logic of an application* The integration of a neural model into the business logic of an application depends on a number of factors. Firstly, the model must be adapted to the target environment, the procedure of such adaptations was described in detail in the preceding steps. Secondly, integrating the model into the application's business logic is a challenging task itself as simply obtaining an optimized model is not enough to deploy it into an application. Therefore, it requires certain competencies and qualifications from application engineers. Lastly, a model cannot be successfully deployed without a runtime environment in which it can be executed efficiently. Provided with the application, the runtime must be able to adapt to the target environment and satisfy business requirements. Since targets can be low-power platforms with limited memory, the model runtime environment should be kept as small as possible. OpenVINO allows to obtain a customized runtime to prepare an application for production.

The adoption of such a methodology provides a detailed justified assessment and preparation of the neural model for deployment. It enables the deployment of models that are not only fast and accurate, but also trustworthy. Following that, we test the methodology on the image classification model.

4 Methodology Evaluation

In the previous section, we proposed a methodology for obtaining high-performance trustworthy neural models. We examined the applicability of current xAI methods to the image classification task of defining a category for an image by associating it with a certain label. To validate the methodology in the context close to real-life conditions, we establish the following business requirements: CPU as the deployment target, 60 frames per second (FPS) as the inferencing performance in the throughput-oriented mode; additionally, we specify that an optimized model cannot be less accurate than the original model by more than 1% (acceptable accuracy drop within 1%).

1. *Model selection* Adhering to the logic of the proposed methodology, we select the efficientnet-b5-pytorch classification model,[1] and the subset of the ImageNet dataset [7] to test it on 1-node 2x Intel(R) Xeon(R) Gold 6240 CPU @ 2.60 GHz (frequency not fixed), Cascade Lake, microcode 0x1, HT off, Turbo off, Ubuntu 18.04.6 LTS, kernel version: 4.15.0-158-generic. Example results of the selected model inference are demonstrated in Fig. 1. After ensuring that the model correctly defines the classes, we proceed to the next step.



ⓘ Drag and drop or upload an image and select visualization type to visualize the model output.

Visualization Type: Model Predictions

ⓘ Model predictions with corresponding confidence levels.

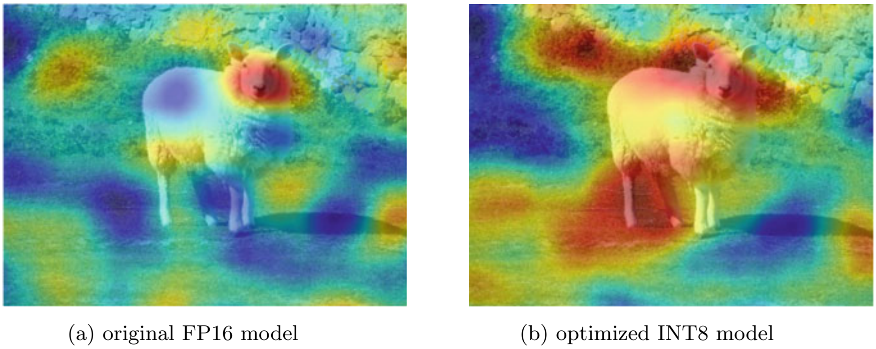
Fig. 1 The model has been tested in the DL Workbench; its highest confidence level prediction matches the object in the example image: #348 ram

[1] https://github.com/rwightman/gen-efficientnet-pytorch.

2. *Runtime environment selection* We need to select the runtime environment considering the business requirements that determine the usage of a CPU device. The OpenVINO framework enables to get accelerated performance for CPU devices and includes a comprehensive graphical interface (DL Workbench). Other frameworks propose similar solutions, for example, Tensorboard [11] or DLProf [16]; however, they are less focused on analyzing and preparing the model for deployment. We select OpenVINO (2021.4.2 version) as the runtime environment and the DL Workbench [6] as the analytical platform.
3. *Evaluation of model performance characteristics* After selecting the model and converting it to IR format, we proceed to assess our model inferencing and accuracy performance. Receiving the results (see Table 1), we can conclude that the model has an inferencing performance of 36.6 FPS in throughput-oriented mode, and 15.08 FPS in latency-oriented mode. With regards to accuracy, model demonstrates accuracy performance of 91.0 %.
4. *Evaluation of model trustworthiness* Next, we need to ensure that the model's predictions can be trusted. For that, we use a representative image and apply the xAI method. Example results of the saliency map for the original model are demonstrated in Fig. 2a. In the image, we can observe that the object's most significant characteristic (ram's head) served as the classification basis. Since the model

Table 1 Original and optimized efficientnet-b5-pytorch model metrics

Characteristics	Original model	Optimized model
Precision	32-bit floating point	8-bit integer
Model size (Mb)	121.9	32.8
Latency-oriented performance (FPS)	15.08	35.54
Throughput-oriented performance (FPS)	36.66	79.04
Accuracy (%)	91.0	90.5



(a) original FP16 model

(b) optimized INT8 model

Fig. 2 xAI method

makes confident and accurate decisions, we can define it as trustworthy. Nevertheless, the model does not meet the requirements for inferencing performance. According to the proposed methodology, we proceed to Step 5 to accelerate the performance.

5. *Model optimization* The inferencing performance is the only parameter that does not satisfy the requirements. Since we selected OpenVINO as a runtime and a CPU target that supports 8-bit integer quantization, we optimize the model using INT8 calibration with the default method and performance preset configurations in the post-training optimization tool.
6. *Post-optimization performance characteristics assessment* As a result, we obtained an improved version of the model. To confirm this, we compare the obtained results to the original model (see Table 1). We observe that the optimized model has become 2.3x faster in terms of latency-oriented performance, and 2.2x faster in throughput-oriented mode. The size of the optimized model has decreased by 3.7x times compared to the original model. Analyzing the primary performance characteristics of the model, we conclude that the inferencing performance (79.04 FPS) has been significantly improved and fully satisfies the requirements. While accuracy performance has been reduced by 0.5 %, it also meets the business requirements. Following the methodology, our next step is to examine the decision-making process of the optimized model.
7. *Evaluation of model trustworthiness after optimization* To assess the prediction trustworthiness of the optimized model, we utilize the xAI technique on the same representative image. Example results of the saliency map for the optimized model are demonstrated in Fig. 2b. We can observe that the model's focus on certain pixels has become more dispersed. At this step, application engineers need to decide whether such a difference in the decision-making process is acceptable. In case of unacceptable results, we recommend returning to Step 5 and applying other optimization configurations. If the difference is acceptable, and the optimized model is trustworthy, we proceed to the next step.
8. *Integrating the model into the business logic of an application* At the last step, to integrate the model into the business logic, we wrote a sample application using OpenVINO Python or C++ API, for example, inside the Jupyter notebook running alongside with the Deep Learning Workbench in the same Docker container. It is also possible to obtain a snapshot of OpenVINO runtime with a help of DL Workbench in a form of deployment package. The size of the bundle containing necessary binaries for efficient execution of models on CPU targets is 14.1 Mb (in a form of ZIP archive).

5 Conclusion

In this paper, we introduced a methodology that pays particular attention to pretrained model's trustworthiness during its preparation for deployment. The methodology helps users comprehend, test, and improve deep learning models while maintaining a high level of performance and accuracy. We have evaluated the methodology on the specified business requirements and obtained a fast and trustworthy model, ready for deployment into a business application. We tested the methodology on a classification model, and one of the important potential directions of the research is to evaluate the applicability of the methodology in other business scenarios, such as object detection and segmentation use cases.

Disclaimers

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex. No product or component can be absolutely secure. Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy. Your costs and results may vary. Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade. Intel technologies may require enabled hardware, software or service activation.

©Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of other

References

1. Alvarez-Melis D, Jaakkola TS (2018) On the robustness of interpretability methods. arXiv preprint arXiv:1806.08049 (2018)
2. Amazon: Amazon SageMaker clarify (2021) Accessed 24 Nov 2021. https://docs.aws.amazon.com/sagemaker/latest/dg/sagemaker-dg.pdf#clarify-model-explainability
3. Chen S, Zhao Q (2018) Shallowing deep networks: layer-wise pruning based on feature representations. IEEE Trans Pattern Anal Mach Intell 41(12):3048–3056
4. Chen T, Moreau T, Jiang Z, Zheng L, Yan E, Shen H, Cowan M, Wang L, Hu Y, Ceze L et al (2018) {TVM}: an automated end-to-end optimizing compiler for deep learning. In: 13th {USENIX} symposium on operating systems design and implementation ({OSDI} 18), pp 578–594
5. Demidovskij A, Tugaryov A, Fatekhov M, Aidova E, Stepyreva E, Shevtsov M, Gorbachev Y et al (2022) Accelerating object detection models inference within deep learning workbench. In: 2021 IEEE 7th international conference on engineering and emerging technologies (ICEET) (in print). IEEE
6. Demidovskij A, Tugaryov A, Suvorov A, Tarkan Y, Fatekhov M, Salnikov I, Kashchikhin A, Golubenko V, Dedyukhina G, Alborova A et al (2020) Openvino deep learning workbench: a platform for model optimization, analysis and deployment. In: 2020 IEEE 32nd international conference on tools with artificial intelligence (ICTAI). IEEE, pp 661–668
7. Deng J, Dong W, Socher R, Li LJ, Li K, Fei-Fei L (2009) Imagenet: A large-scale hierarchical image database. In: 2009 IEEE conference on computer vision and pattern recognition. Ieee, pp 248–255

8. Ding R, Liu Z, Blanton RS, Marculescu D (2018) Quantized deep neural networks for energy efficient hardware-based inference. In: 2018 23rd Asia and South Pacific design automation conference (ASP-DAC). IEEE, pp 1–8
9. European Commission High-Level Expert Group: The OECD principles on artificial intelligence promote artificial intelligence (2019) (Accessed 24 Nov 2021). https://www.oecd.org/going-digital/ai/principles/
10. European Union: general data protection regulation (2018) (Accessed 24 Nov 2021). https://gdpr-info.eu/
11. Google: TensorBoard: tensorFlow's visualization toolkit (2016) (Accessed 24 Nov 2021). https://www.tensorflow.org/tensorboard
12. Google: vertex explainable AI (2021) (Accessed 24 Nov 2021). https://cloud.google.com/explainable-ai
13. Linardatos P, Papastefanopoulos V, Kotsiantis S (2021) Explainable Ai: a review of machine learning interpretability methods. Entropy 23(1):18
14. Lundberg SM, Lee SI (2017) A unified approach to interpreting model predictions. In: Proceedings of the 31st international conference on neural information processing systems, pp 4768–4777
15. Microsoft: model interpretability in Azure Machine Learning (2021) (Accessed 24 Nov 2021). https://docs.microsoft.com/en-us/azure/machine-learning/how-to-machine-learning-interpretability
16. NVIDIA: deep learning profiler (DLProf) (2019) (Accessed 24 Nov 2021). https://docs.nvidia.com/deeplearning/frameworks/dlprof-user-guide/
17. NVIDIA: NVIDIA TensorRT 8.2.1 (2021) (Accessed 24 Nov 2021). https://developer.nvidia.com/tensorrt/
18. OpenVINO: deep learning accuracy validation framework (2018) (Accessed 24 Nov 2021). https://docs.openvino.ai/latest/omz_tools_accuracy_checker.html
19. OpenVINO: open model Zoo (2018) (Accessed 24 Nov 2021). https://docs.openvino.ai/latest/model_zoo.html
20. OpenVINO: post-training optimization toolkit (2020) (Accessed 24 Nov 2021). https://docs.openvino.ai/latest/index.html
21. OpenVINO: OpenVINO 2021.4.2 (2021) (Accessed 24 Nov 2021). https://github.com/openvinotoolkit/openvino
22. Petsiuk V, Das A, Saenko K (2018) Rise: randomized input sampling for explanation of black-box models. arXiv preprint arXiv:1806.07421
23. Ribeiro MT, Singh S, Guestrin C (2016) "Why should i trust you?" explaining the predictions of any classifier. In: Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining, pp 1135–1144
24. Selvaraju RR, Cogswell M, Das A, Vedantam R, Parikh D, Batra D (2017) Grad-cam: visual explanations from deep networks via gradient-based localization. In: Proceedings of the IEEE international conference on computer vision, pp 618–626
25. Slack D, Hilgard S, Jia E, Singh S, Lakkaraju H (2019) How can we fool lime and shap? Adversarial attacks on post hoc explanation methods
26. The alliance in the field of artificial intelligence: the code of ethics in the field of AI (2021) (Accessed 24 Nov 2021). https://a-ai.ru/code-of-ethics
27. The Government of Canada: directive on automated decision-making (2019) (Accessed 24 Nov 2021). https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592
28. The national governance committee for the new generation artificial intelligence: ethical norms for new generation artificial intelligence (translation to eng) (2021) (Accessed 24 Nov 2021). https://ai-ethics-and-governance.institute/2021/09/27/the-ethical-norms-for-the-new-generation-artificial-intelligence-china
29. The White House: national artificial intelligence initiative act of 2020 (2020) (Accessed 24 Nov 2021). https://www.congress.gov/bill/116th-congress/house-bill/6216

A Review of a Research in 2021 on Coronavirus Disease (COVID-19) in Pediatric Patients

Burcu Kir Savaş

Abstract *Background* Although there were other reviews in 2019 and 2020, this is the first review of research that summarizes clinical features of the children with COVID-19 mentioned in literature in 2021. This paper analyses the findings on COVID-19 infection in children in three countries. *Objective* The purpose of this paper is to review publications using chest CT scans and chest X-ray findings for children with COVID-19 in 2021. *Materials and methods* Studies on COVID-19 for articles presenting scan findings in children with COVID-19 have been included in this review. This review focused on articles including 0 < age and age < 18 years using descriptive statistics to identify patterns including duration and several symptoms of the disease, and their relationship with outcomes. *Results* 12 research articles (n = 6212 children) based on chest CT scans and chest X-ray have been examined. The main results of this review article are as follows: (i) Approximately 1728 (27.81%) of pediatric patients with COVID-19 had normal chest CT scans and chest X-ray images. (ii) The most frequently detected parenchymal lesion was ground glass opacity (GGO) and also bilateral lesions were the common signs of lung lesions. (iii) The lung CT scan findings in children with COVID-19 were less severe than in adult patients.

Keywords COVID-19 on pediatric patients · Machine learning · CT scan/X-ray · Survey

1 Introduction

An epidemic of coronavirus disease (COVID-19) emerged in China in December 2019, infecting people all around the world except Antarctica, and has changed the world dramatically. Then many regions and countries have been affected globally and this disease has been regarded as pandemic [1]. According to the World Health Organization (WHO), as of July 2021, there are 190 million cumulative cases globally

B. K. Savaş (✉)
Kocaeli University Umuttepe Campus, 41001 Kocaeli, Turkey
e-mail: burcu.kir@kocaeli.edu.tr

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_70

of which 4.9 million were reported by the end of July, and there are more than 4 million cumulative deaths by the middle of July [2]. According to statistics, the fact is that if infected cases are not isolated/treated, COVID-19 can easily spread and infect many people. Medical imaging is extremely useful for the treatment of disease and has been highly preferred during clinical trials during the pandemic process. Chest CT/X-rays [3], can play a significant supplementary role in the assessment of COVID-19 complications. Because of high precision and accessibility, chest CT scan plays a magnificent role in the identification of COVID-19 and has been recognized as the most sensitive imaging modality to detect complications [4]. The majority of patients affected with COVID-19 disease have chest CT and chest X-rays abnormality and hence researchers prefer chest CT scans and chest X-rays to be used for early detection of COVID-19 and monitoring the progression of the disease progression. Although X-rays can view only one thing at limited viewing ranges, CT scans can take multiple images in a series. Therefore, it seems when research has been examined, CT scans of the patients are more important than X-ray results [5, 6]. At the early stage of its spread, COVID-19 mostly affected adults and old people; however, children were less influenced by the COVID-19 disease. The chest CT scan approach has some risks like need for sedation, radiation effect, etc. Considering these reasons, this approach cannot be easily preferred for children. In addition, infection complication factor for viral lower respiratory tract in children is lower than in adults therefore it is hugely challenging to determine COVID-19 at the early stage. Only a few studies have investigated COVID-19 in pediatric field. However, the number of children infected is increasing. It is accepted that the majority of pediatric cases are quiescent or asymptomatic but still children get infected by COVID-19 [7] and they have suffered from this virus. Also, it is still disputed that children become heavy spreaders during this process [8]. In March, 2020 which is the first COVID-19 case was reported from Turkey, and, the COVID-19 virus continued to spread in the world. COVID-19 diagnoses of pediatric patients is much like in adults. Despite the worldwide spread, clinical patterns of COVID-19 in pediatric patients still remain largely unclear [9].

This research review is mainly about CT/X-ray imaging finding in children while highlighting the value of radiology research of COVID-19 in pediatric patients. Inspired by this limitation of the research of ML-based [10] pediatric patients of COVID-19 diagnosis, various research has been conducted between January 2021 and November 2021. The contributions of this article are as follows: (1) A comprehensive review has been done examining research based on ML techniques in COVID-19 disease and they were categorized. (2) A comparison of articles has been provided in terms of their application, author, dataset size, laboratory parameters, and study results to provide valuable insights for pediatric cases. (3) This review provides a literature base for future research and fills the gap for understanding contribution from research in 2021 on COVID-19.

2 Infection in Children

According to Pediatric Healthcare Providers, on December 30, 2020, globally fewer reports of COVID-19 have been listed in children between the ages 0–17 as with adults. 22% of the US population consists of children [11, 12]. For the Pediatric Healthcare Providers, recent data show that COVID-19 is more prevalent among children in the United States than people think [13]. In August 2021, the estimated number of patients in children in the United States appears to have increased [14]. The incidence of COVID-19 disease in children is not truly understood because of the lack of generalized reports and the prioritization of testing for adults with COVID-19 disease. Latest data indicate that compared to adults, children most probably have a very much alike viral disease, [15] and can transmit the virus to other people [16, 17]. Preliminary statistics show that children have not been affected seriously by SARS-CoV-2 and less spread the virus because most of the countries were closed school early and parents struggle to protect their children therefore researchers still investigate to not affected children during the pandemic period. On the other hand, the rapid infectious of the disease by children have a significant role in the rapid contamination of the disease among human, so early detection of COVID-19 in children will help reduce the spread in both children and adults. Also, most countries in the world entered the new normalization process in the autumn of September 2021. In this process, when most of the schools and daycares reopened, understanding transmission potential in children will be important to guide public health measures. Children's incubation period of COVID-19 is considered the same as in adults, at 2–14 days with a standard of 6 days [18]. Signs of COVID-19 in children are as follows: cough, fever, sore throat, myalgia, abdominal pain, loss of taste, loss of smell, headache, difficulty breathing, diarrhea nausea or vomiting, and poor appetite [19]. Most children may have all signs or some of these symptoms when they are infected with COVID-19. Although these symptoms in children similar to adults are considered, lack of statistics of symptoms or originality of signs for recognition or classification COVID-19 in children is especially challenging [20].

3 Methods and Included Studies

Twelve studies are analyzed from research articles published on COVID-19 from January 2021 to November 2021 using the keywords COVID-19, children, pediatrics, SARS-CoV-2, Epidemiology, Guidelines, Audio/Speech, CT Scan, X-ray images. This research focused on clinical journal articles and case reports/series. All journal articles and case reports written in English were analyzed and criticized. Also, the preprints have been examined due to the lack of COVID-19 statistics in children.

In this section, the scope of each review such as topics, types, interests, and architecture of the study are examined. The criteria of the present review are shown in Table 1 and pediatric COVID-19 cases included in the results and nation Table 2.

Table 1 Present research criteria

	Criteria	Focused on / eliminate
Researches	Pediatric cases	Clinical journal articles, case reports/series/thesis
Population	Children age <18, for both genders, in Asian, USA, and Europe	COVID-19 disease and symptoms/Specific disorders and diseases
Measurement parameters	ML techniques	CT and X-ray images

Among 74 children has right-sided (4.3%) or bilateral (4.3%) GGO and also feeding vessel sign, halo sign, and pleural thickening [21]. In 1156 children did biochemical tests and complete blood count and chest CT/X-ray. Among these children, 263 have (22.7%) asymptomatic, 668 have (57.7%) mild disease, 209 have (18.1%) moderate disease, and 16 have (1.5%) severe disease [22]. Among 422 children, 23 have (29.5%) asymptomatic, 45 have (56.4%) mild disease, 10 have (12.9%) moderate, 1 have (1.2%) severe, and 0% critical cases [23]. Among 148 children CT finding was classified that 52 PCR positive patients and regarding CT finding 23 PCR positive and 12 negative patients, approximately (65%) unilateral, approximately (51%) multifocal, approximately (88%) peripheral, and approximately (61%) lower lobe involvement [24]. Among 177 children, 79 have (44.6%) bone lesions, 98 have (55.4%) normal [5]. Among 40 children result for chest CT; good sensitivity, GGO sub-pleural basal, nodular consolidation not frequent, peribronchial thickening frequent, pleural effusion possible, for chest X-ray result; low sensitivity, GGO sub-pleural basal, nodular consolidation not frequent, peribronchial thickening frequent, pleural effusion possible [25]. Among 3670 children, 1026 (36\%) was normal and 798 (28%) bilateral lesions, 1054 (37%) GG0 and consolidation or pneumonic infiltrates 22% [26]. Among 24 children, 7 (33%) was normal, 8 (38%) had patchy or streaky opacity, GGO geographic, 1 (5\%) had dense opacity, 3 (14%) had bronchial wall thickening, 1 (5%) had hyperinflation, 1 (5%) had wedge-like opacity, 2 (10%) had pleural effusion [27]. Among 47 children, 37/45 (82%) had pulmonary opacities (most often bilateral and diffuse), 8/45 (18%) were normal [28]. Among 16 children, 11 (69%) demanded ICU, 10 (63%) had hypotension or shock, 7 (44%) had hypoxia, 1 (6%) had intubation and mechanical ventilation [29]. Among 16 children, 4 (25%) had typical, 8 (50%) had indeterminate, 1 (6%) was atypical, 3 (19%) had negative [30]. Among 422 children, $n = 95$ patients between ages are 0–19 with PCR test positive for clinical presentation. They subdivided their study group according to age groups including $n = 27$ patients 0–2 years of infants, $n = 27$ patients 3–10 years of children, and $n = 41$ patients 11–19 years of adolescents. 45% of pediatric patients were hospitalized, of which 20% needed acceptance to ICU. The detected abnormalities identified were 35% GGO/consolidations. Also, they remarked GGO/consolidations were more common in older people than younger people [31].

Pediatric COVID-19 cases distribution on gender and patient symptoms are given in Table 3. With 2996 (50.79%) males and 2889 (49.20%) females, the 12 eligible

Table 2 Pediatric COVID-19 cases included in the results and nation

Authors	Data count/nation/laboratory/parameters	Results
Bayramoglu et al. [21]	74, Turkey, chest CT/X-ray	Right-sided (4.3%) or bilateral (4.3%) GGO. Feeding vessel sign, halo sign, and pleural thickening
Karbuz et al. [22]	1156, Turkey biochemical tests, complete blood count, chest CT/X-ray	*n* = 263 (22.7%) asymptomatic, *n* = 668 (57.7%) mild disease, *n* = 209 (18.1%) moderate disease, and *n* = 16 (1.5%) severe disease
Berksoy et al. [23]	422, Turkey, chest CT/X-ray	*n* = 2 (29.5%) asymptomatic, *n* = 45 (56.4%) mild, *n* = 10 (12.9%) moderate, *n* = 1 (1.2%) severe, and critical cases *n* = 0 (0%)
Kalin et al. [24]	148, Turkey, chest CT/X-ray	CT finding was classified (23 PCR positive and 12 negative patients), (61–67%) unilateral, (50–52%) multifocal, and (83–91%) peripheral, (58–65%) lower lobe involvement, the most frequently detected parenchymal lesion was GGO followed by consolidated areas accompanying ground-grass opacities, (35%) halo sign and vascular enlargement signs, using CXR for control radiological imaging
Bottari et al. [5]	177, Italy, bone CT/ X-ray, ultrasound	*n* = 79 (44.6%) bone lesions, *n* = 98 (55.4%) normal
Ferrero and Piazza [25]	40, Italy, chest CT/X-ray	CT: good sensitivity, GGO sub-pleural basal, nodular consolidation not frequent, peribronchial thickening frequent, pleural effusion possible. X-ray: low sensitivity, GGO sub-pleural basal, nodular consolidation not frequent, peribronchial thickening frequent, pleural effusion possible
Deville et al. [26]	3670, US, chest CT/X-ray	*n* = 1026 (36%) normal and *n* = 798 (28%) bilateral lesions, *n* = 1054 (37%) GG0 and consolidation or pneumonic infiltrates 22%

(continued)

Table 2 (continued)

Authors	Data count/nation/laboratory/parameters	Results
Romberg et al. [27]	24, US, chest CT/X-ray	$n = 7$ (33%) normal, $n = 8$ (38\%) patchy or streaky opacity, GGO geographic, $n = 1$ (5%) dense opacity, $n = 3$ (14%) bronchial wall thickening, $n = 1$ (5%) hyperinflation, $n = 1$ (5%) wedge-like opacity, $n = 2$ (10%) pleural effusion
Fenlon et al. [28]	47, US, chest CT/X-ray, MRI	$n = 37/45$ (82%) pulmonary opacities (most often bilateral and diffuse), $n = 8/45$ (18%) normal
Blumfield et al. [29]	16, US, chest CT/X-ray, ultrasound	$n = 11$ (69%) admission ICU (PICU), $n = 10$ (63\%) hypotension or shock. $N = 7$ (44%) hypoxia, $n = 1$ (6%) intubation and mechanical ventilation
Rostad et al. [30]	16, US, chest CT/X-ray	$n = 4$ (25%) typical, $n = 8$ (50\%) indeterminate, $n = 1$ (6%) atypical, $n = 3$ (19%) negative
Nino et al. [31]	422, US, chest X-ray	$n = 95$ PCR positive patient, $n = 49$ (52%) abnormal findings, $n = 33$ (35%) GGO/consolidations, $n = 16$ (17%) multifocal GGO/consolidations, $n = 0.46$ (0.8%) lung zones affected, $n = 6$ (6%) hyperinflation, $n = 32(34)$ increased peribronchial markings/cuffing, $n = 1(1\%)$ air bronchogram, $n = 4$ (4%) pleural effusion

Note *CT* Computed tomography, *X-Ray* electromagnetic radiation, *GGO* ground glass opacity, *n*: patients with COVID-19, *typical* chest, radiograph findings, *indeterminate* nonspecific chest radiograph findings, *atypical* radiograph findings that are uncommon or not reported, *negative* no chest radiographic findings of pediatric pneumonia, *US* United States

studies were from 3 different countries. 4 (33.33%) were from Turkey [21–24], including 2 (16.66%) from Italy [5, 25] and 6 (50%) from the US [26–31]. Among the 12 included studies, one (8.3%) was a case report [25], 10 (83.3%) were original research articles [5, 21, 22, 24, 26–31], and one (8.3%) was a brief report [5]. Except for these studies, there are 7 other studies in COVID-19 with different perspectives for pediatric cases [32–39].

Table 3 Pediatric COVID-19 cases for gender group and other symptoms

Authors	Gender group	Other symptoms
Bayramoglu et al. [21]	Male:36 female:38	Fever, cough, diarrhea, hypotension, loss of taste, dyspnea, loss of smell, myalgia
Karbuz et al. [22]	Male:582 female:574	Cough (543/1156 46.9%), fever (583/1156 50.4%), throat (143/1156 12.4%), myalgia (141/1156 12.2%), dyspnea (118/1156 10.2%), diarrhea (112/1156 9.7%) stomachache (71/1156 6.1%), and nasal discharge (63/1156 5.4%)
Berksoy et al. [23]	Male:243 female:179	Fever (258/164 51.2%), cough (269/153 43.5%), sore throat (43/379), rhinorrhea (25/397), diarrhea (32/389), nausea-vomiting (34/388). Others (headache, malgia, weakness, etc.) (76/346), Tachypnea (167/251)
Kalin et al. [24]	Male:78 female:70	Cough (30/52 57.7%), respiratory distress (22/52 42.3%), fever (11/52 21.2%), sore throat (8/52 15.4%), GIS symptoms (7/52 13.5%), joint findings (6/52 11.5%), headache (5/52 9.6%), fatigue (3/52 5.8%), loss of taste and smell (2/52 3.8%), comorbid disease (8/52 15.4%), hospitalization (33/52 63.5%)
Bottari et al. [5]	Male:100 female:77	29 images upper limbs, 22 images lower limbs, 42 images axial bones
Ferrero and Piazza [25]	Male and female:40	Multi-system inflammatory syndrome
Deville et al. [26]	Male and female:3670	Fever (63.3%), cough (33.7%) and multi-system inflammatory
Romberg et al. [27]	Male:11 female:13	$n = 2$ pulmonary embolism in setting of tachypnea and tachycardia and fevers/sepsis, $n = 2$ mild septal thickening
Fenlon et al. [28]	Male:22 female:25	Multi-system inflammatory, fever, hypotensive shock, chest pain, dyspnea, cough
Blumfield et al. [29]	Male:10 female:6	Fever (100%), vomiting (12/16, 75%), abdominal pain (11/16, 69%), rash (10/16, 63%), conjunctivitis (8/16, 50%), diarrhea (7/16, 44%), headache (6/16, 38%), and sore throat (5/16, 31%)
Rostad et al. [30]	Male:10 female:6	Cough (13/16, 81%), fever (14/16, 88%), vomiting (8/16, 50%), abdominal pain (1/16, 6%), myalgia (2/16, 13%), dyspnea (6/16, 38%), chest pain (3/16, 19%), headache (3/16, 19%), diarrhea (4/16, 25%), and sore throat (3/16, 19%)
Nino et al. [31]	Male:49, female:46	–

4 Discussion

Many studies have focused on the fact that it is difficult to distinguish the diagnosis of COVID-19 from the diagnosis of non-COVID-19 diseases such as influenza or pneumonia. These studies have determined that various medical data (X-ray/CT images) are used for the diagnosis of COVID-19. However, since it is very difficult to understand the difference between the symptoms of COVID-19 disease and the symptoms of other diseases, it can cause misdiagnosis [39]. As a result of the misdiagnosis, many negative situations such as malpractice and wrong drug use can occur or it can cause permanent damage to patients. Hence, it is very important to have a mature, robust, and integrated system [40] that automatically detects the COVID-19 disease. It has been observed that the majority of studies in the pediatric field were conducted by researchers in the USA and Turkey. In addition, it is thought that there is an urgent need to conduct more studies on this subject.

5 Conclusion

COVID-19 is a contagious disease that has quickly endangered the health of humanity as a global pandemic. Due to this disease, this world is affected as communal, cultural, and economic. Even though COVID-19 mostly affects adults, children are affected by COVID-19 disease in many ways. This comprehensive review summarizes the clinical features of children with COVID-19 in 2021. Currently, most of the result of evidence results from studies and cases from China. However, the spread of COVID-19 disease accelerate worldwide, and because of the lack of European and US data on pediatric patients need further clinical cases to identify possible preventive scenarios. Also, it is fact that more research is still a requirement to understand how COVID-19 has affected children and to produce treatments and productive vaccines for children. In this research, the effects of COVID-19 on children in 2021 have examined, published and listed. Many children in pediatric patients have a mild course. Therefore, a balance between the risk of radiation and the vitalism for CT scan is very important.

References

1. WHO Director-General's Statement on IHR Emergency Committee on Novel Coronavirus (2019-nCoV). https://www.who.int/dg/speeches/detail/who-director-general-s-statement-on-ihr-emergency-committee-on-novel-coronavirus-(2019-ncov). Accessed 2021/05/01
2. Weekly epidemiological update on COVID-19—20 Jul 2021. https://www.who.int/publications/m/item/weekly-epidemiological-update-on-covid-19---20-july-2021. Accessed 2021/08/01
3. Borakati A, Perera A, Johnson J, Sood T (2020) Diagnostic accuracy of X-ray versus CT in COVID-19: a propensity-matched database study. BMJ Open 10(11)

4. Sun Z, Zhang N, Li Y, Xu X (2020) A systematic review of chest imaging findings in COVID-19. Quant Imaging Med Surg 10(5):1058
5. Bottari G, Stellacci G, Ferorelli D, Dell'Erba A, Aricò M, Benevento M, Palladino G, Solarino B (2021) Imaging appropriateness in pediatric radiology during COVID-19 pandemic: a retrospective comparison with no COVID-19 Period. Children 8(6):463
6. Bai HX, Hsieh B, Xiong Z, Halsey K, Choi JW, Tran TML, Pan I, Shi LB, Wang DC, Mei J, Jiang XL, Liao WH (2020) Performance of radiologists in differentiating COVID-19 from non-COVID-19 viral pneumonia at chest CT. Radiol 296(2):E46–E54
7. Riphagen S, Gomez X, Gonzalez-Martinez C, Wilkinson N, Theocharis P (2020) Hyperinflammatory shock in children during COVID-19 pandemic. The Lancet 395(10237):1607–1608
8. Cao Q, Chen YC, Chen CL, Chiu CH (2020) SARS-CoV-2 infection in children: transmission dynamics and clinical characteristics. J Formos Med Assoc 119(3):670
9. Jin XM, Xu X (2013) The society of pediatrics, Chinese Medical Association-an intensive training programme for developmental and behavioral pediatrics. Zhonghua er ke za zhi= Chin J Pediatr 51(11):879–880
10. Shi F, Wang J, Shi J, Wu Z, Wang Q, Tang Z, He K, Shi Y, Shen D (2020) Review of artificial intelligence techniques in imaging data acquisition, segmentation, and diagnosis for COVID-19. IEEE Rev Biomed Eng 14:4–15
11. Stokes EK, Zambrano LD, Anderson KN, Marder EP, Raz KM, Felix SEB, Tie Y, Fullerton KE (2020) Coronavirus disease 2019 case surveillance—United States, 22 Jan–30 May, 2020. Morb Mortal Wkly Rep 69(24):759
12. Williams N, Radia T, Harman K, Agrawal P, Cook J, Gupta A (2021) COVID-19 severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) infection in children and adolescents: a systematic review of critically unwell children and the association with underlying comorbidities. Eur J Pediatr 180(3):689–697
13. U.S. Census Bureau. Quick Facts United States. https://www.census.gov/quickfacts/fact/table/US/AGE295219#AGE295219externalicon. Accessed 2021/07/01
14. Centers for Disease Control and Prevention. Demographic trends of COVID-19 cases and deaths in the US reported to CDC. https://www.cdc.gov/covid-data-tracker/index.html#demographics. Accessed 2021/08/01
15. Heald-Sargent T, Muller WJ, Zheng X, Rippe J, Patel AB, Kociolek LK (2020) Age-related differences in nasopharyngeal severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) levels in patients with mild to moderate coronavirus disease 2019 (COVID-19). JAMA Pediatr 174(9):902–903
16. Yonker LM, Neilan AM, Bartsch Y, Patel AB, Regan J, Arya P, Gootkind E, Park G, Hardcastle M, John AS, Appleman L, Fasano A (2020) Pediatric severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2): clinical presentation, infectivity, and immune responses. J Pediatr 227:45–52
17. Laws RL, Chancey RJ, Rabold EM, Chu VT, Lewis NM, Fajans M, Reses HE, Duca LM, Dawson P, Conners EE, Gharpure R, Kirking HL (2021) Symptoms and transmission of SARS-CoV-2 among children—Utah and Wisconsin, March–May 2020. Pediatr 147(1)
18. Centers for Disease Control and Prevention. COVID-19 pandemic planning scenarios. https://www.cdc.gov/coronavirus/2019-ncov/hcp/planning-scenarios.html#table-2. Accessed 2021/08/05
19. Information for Pediatric Healthcare Providers. https://www.cdc.gov/coronavirus/2019-ncov/hcp/pediatric-hcp.html. Accessed 2021/08/05
20. Poline J, Gaschignard J, Leblanc C, Madhi F, Foucaud E, Nattes E, Faye A, Bonacorsi S, Mariani P, Varon E, Smati-Lafarge M, Ouldali N (2021) Systematic severe acute respiratory syndrome coronavirus 2 screening at hospital admission in children: a French prospective multicenter study. Clin Infect Dis 72(12):2215–2217
21. Bayramoglu Z, Canıpek E, Comert RG, Gasimli N, Kaba O, Yanartaş MS, Torun SH, Somer A, Erturk SM (2021) Imaging features of pediatric COVID-19 on chest radiography and chest CT: a retrospective, single-center study. Acad Radiol 28(1):18–27

22. Karbuz A, Akkoc G, Demirdag TB, Ciftdogan DY, Ozer A, Cakir D, Torun SH, Kepenekli E, Erat T, Dalgic N, Ilbay S, Kara A (2021) Epidemiological, clinical, and laboratory features of children with COVID-19 in Turkey. Front Pediatr 9
23. Berksoy E, Kanik A, Çiçek A, Bardak Ş, Elibol P, Demir G, Yilmaz N, Nalbant T, Gökalp G, Yilmaz Çiftdoğan D (2021) Clinical and laboratory characteristics of children with SARS-CoV-2 infection. Pediatr Pulmonol
24. Kalin S, Ciraci S, Cakir D, Oysu AS, Sozeri B, Demir F, Bukte Y (2021) Evaluation of radiological findings in pediatric patients with COVID-19 in Turkey. Northern Clin Istanbul 8(4):332
25. Ferrero P, Piazza I (2021) Cardio-thoracic imaging and COVID-19 in the pediatric population: a narrative review. World J Radiol 13(4):94
26. Deville JG, Song E, Ouellette CP (2021) COVID-19: clinical manifestations and diagnosis in children
27. Romberg EK, Menashe SJ, Kronman MP, Tang ER, Stanescu AL, Otto RK, Otjen JP (2021) Pediatric radiologic manifestations of COVID-19. Clin Imaging 75:165–170
28. Fenlon Iii EP, Chen S, Ruzal-Shapiro CB, Jaramillo D, Maddocks AB (2021) Extracardiac imaging findings in COVID-19-associated multisystem inflammatory syndrome in children. Pediatr Radiol 51(5):831–839
29. Blumfield E, Levin TL, Kurian J, Lee EY, Liszewski MC (2021) Imaging findings in multisystem inflammatory syndrome in children (MIS-C) associated with coronavirus disease (COVID-19). Am J Roentgenol 216(2):507–517
30. Rostad BS, Shah JH, Rostad CA, Jaggi P, Richer EJ, Linam LE, Alazraki AL, Riedesel EL, Milla SS (2021) Chest radiograph features of multisystem inflammatory syndrome in children (MIS-C) compared to pediatric COVID-19. Pediatr Radiol 51(2):231–238
31. Nino G, Molto J, Aguilar H, Zember J, Sanchez-Jacob R, Diez CT, Tabrizi PR, Mohammed B, Weinstock J, Xuchen X, Kahanowitch R, Linguraru MG (2021) Chest X-ray lung imaging features in pediatric COVID-19 and comparison with viral lower respiratory infections in young children. Pediatr Pulmonol
32. Irfan O, Muttalib F, Tang K, Jiang L, Lassi ZS, Bhutta Z (2021) Clinical characteristics, treatment and outcomes of paediatric COVID-19: a systematic review and meta-analysis. Arch Dis Child 106(5):440–448
33. Adeyinka A, Bailey K, Pierre L, Kondamudi N (2021) COVID 19 infection: pediatric perspectives. J Am Coll Emerg Phys Open 2(1):e12375
34. Shuja J, Alanazi E, Alasmary W, Alashaikh A (2021) COVID-19 open source data sets: a comprehensive survey. Appl Intell 51(3):1296–1325
35. Mamikutty R, Aly AS, Marhazlinda J (2021) Databases selection in a systematic review of the association between anthropometric measurements and dental caries among children in Asia. Child 8(7):565
36. Zang ST, Han X, Cui Q, Chang Q, Wu QJ, Zhao YH (2021) Imaging characteristics of coronavirus disease 2019 (COVID-19) in pediatric cases: a systematic review and meta-analysis. Transl Pediatr 10(1):1
37. Trout AT, Westra SJ (2021) Imaging in support of the clinical diagnoses of COVID-19 and multisystem inflammatory syndrome in children. Pediatr Radiol 51(5):693–694
38. Tulchin-Francis K, Stevens Jr W, Gu X, Zhang T, Roberts H, Keller J, Dempsey D, Borchard J, Jeans K, VanPelt J (2021) The impact of the coronavirus disease 2019 pandemic on physical activity in US children. J Sport Health Sci 10(3):323–332
39. Bayesheva D, Boranbayeva R, Turdalina B, Fakhradiyev I, Saliev T, Tanabayeva S, Zhussupov B, Nurgozhin T (2021) COVID-19 in the paediatric population of Kazakhstan. Paediatr Int Child Health 41(1):76–82
40. Savaş BK, Becerikli Y (2020) Real time driver fatigue detection system based on multi-task ConNN. IEEE Access 8(1):12491–12498

Transferability of Quantum Adversarial Machine Learning

Vincent Li, Tyler Wooldridge, and Xiaodi Wang

Abstract Quantum adversarial machine learning lies at the intersection of quantum computing and adversarial machine learning. As the attainment of quantum supremacy demonstrates, quantum computers have already outpaced classical computers in certain domains (Arute et al. in Nature 574:505–510, 2019 [3]). The study of quantum computation is becoming increasingly relevant in today's world. A field in which quantum computing may be applied is adversarial machine learning. A step toward better understanding quantum computing applied to adversarial machine learning has been taken recently by Lu et al. (Phys Rev Res 2:1–18, 2020 [13]), who have shown that gradient-based adversarial attacks can be transferred from classical to quantum neural networks. Inspired by Lu et al. (Phys Rev Res 2:1–18, 2020 [13]), we investigate the existence of the transferability of adversarial examples between different neural networks and the implications of that transferability. We find that, when the fast gradient sign attacks, as described by Goodfellow et al. (Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572 [9]), is applied to a quantum neural network, the adversarially perturbed images produced with that method have transferability between quantum neural networks and from quantum to classical neural networks. In other words, adversarial images produced to deceive a quantum neural network can also deceive other quantum and classical neural networks. The results demonstrate that there exists transferability of adversarial examples in quantum machine learning. This transferability suggests a similarity in the decision boundaries of the different models, which may be an important subject of future study in quantum machine learning theory.

V. Li (✉) · T. Wooldridge · X. Wang
Western Connecticut State University, 181 White St., Danbury, CT 06810, USA
e-mail: vincent.li.application@gmail.com

X. Wang
e-mail: wangx@wcsu.edu

V. Li
Horace Mann School, 231 W 246 St., Bronx, NY 10471, USA

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_71

Keywords Quantum adversarial machine learning · Fast gradient sign method · Transfer attack · Quantum neural network · Classical neural network · Black box attack

1 Introduction

With the attainment of quantum supremacy [3], researchers and computer scientists have investigated ways for quantum computers to exponentially speed up classical computation. Quantum computers can improve machine learning through quantum machine learning and qubits. Qubit states can go into superposition and be rotated around the x, y, and z axes [8], which sets them apart from classical bits. Two or more qubits can be put into an entangled state. The entangled qubits will become correlated such that when one is measured; the others will collapse to the same state [16].

There are many different techniques and fields of study under the field of machine learning, including neural networks. A neural network is a computational model inspired by biological neurons. Gradient descent is used in machine learning as an optimization algorithm; its goal is to minimize the cost function [17]. Even though, according to [18], "Neural networks and decision trees are still waiting for a convincing quantum version" (p. 2), research in quantum adversarial machine learning has been growing for when these neural networks are possible.

Adversarial machine learning studies the vulnerabilities of machine learning models by analyzing how data can be altered to fool the model into misclassifying it [11]. Models can be made more robust when they are trained with adversarial examples [9], making them less susceptible to attacks. For that reason, it is imperative that these samples be identified. Transfer attacks can be used in the case of black box attacks. Some new developments in quantum adversarial machine learning include the discovery of the transferability of adversarial examples from classical neural networks to quantum neural networks [7].

Although the discovery of transferability [7] is quite significant, much is still unknown, such as whether "No-Free Lunch" theorem [13] (a general-purpose universal optimization strategy is not possible [2]) applies to quantum machine learning. In this paper, we will experiment on and describe the transferability of quantum adversarial examples and determine if an adversarial sample that fools a quantum neural network may also fool other quantum or classical neural networks.

2 Preliminaries and Methods

2.1 Preliminaries

In this study, we used Python [15], TensorFlow Keras [1], TensorFlow Quantum [4], NumPy [10], Scikit-Learn [14], SymPy [19], and Cirq [6]. Matplotlib [5] was used for plotting the figures. In this research, we used the MNIST dataset [12], which consists of 70,000 labeled images (28-by-28, or 784 pixels) of handwritten digits from 0 to 9. The dataset is divided into a training set of 60,000 images and a testing set of 10,000 images.

Quantum Neural Network Design To perform the adversarial attacks and to test the transferability of the adversarial examples, two different quantum neural networks were created. Information about the weights and architecture of the white box quantum neural network was used to construct adversarial examples, while no such information from the black box quantum neural network was used. Our quantum neural network design is inspired by TensorFlow Developers [21]. Both quantum neural networks were parameterized quantum circuits consisting of 17 qubits: 16 data qubits for input data and 1 readout qubit for the output. To prepare the readout qubit, an X gate and an H gate were applied. Following those gates, there were three parameterized layers of gates in the middle, which differed for each quantum neural network. Finally, another H gate was applied, and the readout was measured in the Z basis. Each of the middle layers consisted of a collection of a single type of quantum gate. This quantum gate was applied to pairs of qubits such that the pair contained the readout qubit and a data qubit. Since there were 16 data qubits, and the gate was applied once for every data qubit, there were 16 such gates. Each of these gates was raised to an exponent whose value parameterized the circuit and was learned through training. The architecture of the middle layers was also inspired by TensorFlow Developers [21].

For the white box quantum neural network, the three middle layers consisted of a layer of double-qubit X gates, followed by a layer of double-qubit Z gates, followed by a layer of controlled-NOT (CNOT) gates. In the CNOT layer, each CNOT gate used a data qubit as the control qubit, while the readout qubit was the target qubit. In the black box quantum neural network, the middle three layers consisted of a layer of double-qubit Y gates, followed by a layer of CNOT gates (using a data qubit as the control qubit, and readout qubit as the target qubit), followed by a layer of controlled-Z (CZ) gates.

Classical Neural Network Design To test the transferability of the adversarial examples to classical neural networks, two different classical models were created.

The first of these was the large classical neural network, with 22,273 total trainable parameters. It consisted of five total layers, the first four of which used the rectified linear unit (ReLU) as its activation function. The first layer took in the 16 inputs and thus had 16 neurons, while the next three layers had 100 neurons each. The last layer, consisting of a single neuron, used the sigmoid activation function in order to restrict the output to the interval (0, 1). The second classical neural network was the small classical neural network, with only 363 total trainable parameters. Similar to the large classical neural network, this model's first layer had 16 neurons and an activation function of ReLU, and the final (third) layer had 1 neuron with a sigmoid activation function. However, the second layer, which is analogous to the previous model's middle three layers, only had five neurons, and its activation function was also ReLU.

2.2 Methods

Preprocessing Data

Reduction of Data Complexity We normalized the images' pixel intensity values by dividing them by 255 and then performed principal component analysis (PCA) on the training images to reduce their dimensionality from 784 (28^2). To find a suitable number of principal components to use, we used a classical neural network to classify the ten classes of images after dimensionality reduction. We ultimately chose to use the first 16 principal components, which greatly reduced the necessary computing power while keeping much of the necessary information. Doing so let the classical neural network have an accuracy of 0.9148 and had an explained variance ratio of 0.5942.

We then projected each 784-dimensional testing image vector onto the 16-dimensional eigenspace spanned by the 16 principal components found previously. This was done in order to ensure that the testing process would be rigorous, since this mimicked real-world conditions in which the testing set is unknown when training the model.

To further reduce the computing power needed, we filtered the data to keep only two classes: zero and five from the MNIST database. The labels were then binarized, as we converted five to 0 and zero to 1.

Normalization. Afterward, we linearly normalized the input data to fit it in the interval [0, 1]. After PCA, the training data consisted of 16-dimensional vectors, each of which represented a single image and contained what we call the "coordinates." We performed the normalization process once for each of the 16 coordinates.

For the testing data, we also performed the coordinate-wise normalization, except we applied the same linear transformation as we did for the training data to ensure the rigor of the testing process.

Quantum Circuit Encoding The method we used for encoding the data onto the quantum circuit was inspired by TensorFlow Developers [21]. To do so, we created a circuit of 16 qubits (one per principal component) for each image. By appending an X gate raised to a power equal to the normalized principal component coefficient to the corresponding qubit, the information was encoded into the quantum circuit.

Training and Testing To save training time, the data was pseudo-randomly shuffled, and only the first 500 examples were used. The classical and black box quantum models were trained on 30 epochs, though the white box quantum model only required ten epochs to convergence. The accuracies of the models were evaluated on the testing set.

Fast Gradient Sign Attack The fast gradient sign attack [9] adversarially perturbs an image by adding the signed gradient (scaled by ε) with respect to the original image x of the loss function J on the model parameters θ, the original image, and the label of the image y. Mathematically, this can be expressed as

$$x_{\text{adv}} = x + \varepsilon \cdot \text{sign}(\nabla_x J(\theta, x, y)) \tag{1}$$

where x_{adv} is the adversarial image.

We use the fast gradient sign attack as described in Goodfellow et al. [9] with a small modification: rather than directly perturbing the original image, we perturbed the PCA coefficients representing the image. This allowed us to calculate gradients with respect to the 16-dimensional PCA coefficient vectors, rather than the 784-dimensional original image vectors. This was done to reduce the computational cost and increase the effectiveness of the attack, as it directly affected the inputs to the neural networks. We also only performed this attack on 500 random images in the testing set, as the gradient calculation was computationally intensive. Our method for computing the gradients of the white box quantum neural network was guided by TensorFlow Developers [20, 22].

Transfer Attack As noted by Lu et al. [13], adversarial attacks often have transferability, meaning that an adversarial example capable of deceiving a classifier can also fool a different classifier, even if these classifiers have different architectures. This transferability means that black box attacks on a victim model can be conducted by performing a white box attack on a model with known parameters first, and then exploit the transferability of the adversarial examples to deceive the victim. In this study, we performed the fast gradient sign attack on the white box quantum neural network. In doing so, we created a set of adversarially perturbed images. Then, we studied the degree to which those adversarially perturbed images fooled the black box quantum neural network and the classical neural networks. We refer to the use of those adversarially perturbed images to attack the black box quantum neural network and the classical neural networks as the "transfer attack."

3 Experimental Results

3.1 Fast Gradient Sign Attack

Some of the gradients of the loss function on the white box quantum neural network were 0 vectors. With 0 gradient, the fast gradient sign attack would not alter the image and hence would be useless. Therefore, we removed the images with 0 gradient; they are not considered in the calculation of accuracy. 67 such images were removed out of the 500 total images in the test set. After the images with 0 gradient were removed, they left behind a set that we will refer to as the "truncated testing set." We refer to the adversarially perturbed truncated testing set as the "adversarial set."

To ensure that the fast gradient sign attack was effective, we experimented with different values of ε. We used the mean cosine similarity as a measure of similarity between the truncated testing and the adversarial sets. This measure was inspired by Lu et al. [13], who used mean fidelity for the same purpose.

3.2 Transfer Attack

Below are the results for the transfer attack on all the black box neural networks.

Accuracy

Confusion Matrices In the following confusion matrices, the classes kept were zero and five.

With $\varepsilon = 0.9$, the large classical neural network's accuracy has settled at around 0.4758, which is not significantly different from chance. Because the model was measured to have similar accuracy levels for each $\varepsilon \geq 0.3$, this confusion matrix is generally representative of the model's predictions under that condition, even for different values of ε. The mean cosine similarity is 0.2627. It is interesting to note that, on the actual positives, the accuracy was 0.0235, which is significantly ($p <$ 0.05) lower than chance.

In Table 1, the model may appear to have predictions whose accuracies make the predictions seem approximately random. However, the confusion matrix reveals that it is not the case: If the predictions were close to random, then there would be roughly equal numbers of predicted positives and negatives. However, this is not the case because there are significantly ($p < 0.05$) more predicted negatives than predicted positives, implying that the transfer attacks have succeeded in forcing the model to predict negatives, thus increasing the false negative count. Furthermore, in that table, the accuracy on the actual positives is also significantly ($p < 0.05$) lower than chance.

Transferability We calculate the transferability ratio the same way as [13]: let $\alpha_{\text{test}}, \alpha_{\text{adv}}$ be the accuracy of the model on the truncated testing and adversarial sets, respectively. The transferability ratio is defined as $\alpha_{\text{test}} - \alpha_{\text{adv}}$, representing the proportion of images for which the adversarial attack was able to cause misclassification. Below is a table of the maximum transferability ratios achieved for all the models (Table 2).

These transferability ratios were evaluated on the classes zero and five. Note that for the white box quantum neural network, the ratio is not truly a transferability

Table 1 Confusion matrix for the large classical neural network for $\varepsilon = 0.9$

$N = 433$	Predicted positives	Predicted negatives
Actual positives	0.0115 (5)[a]	0.4804 (208)
Actual negatives	0.0439 (19)	0.4642 (201)

[a] We list the data as a ratio first, and then the actual number of data points second (in parentheses)

Table 2 Maximum transferability ratios of the attack to each model

Victim classifier	Testing accuracy	Minimum adversarial accuracy	Maximum transferability ratio	ε value
White box quantum neural network	0.9030	0.0577	0.8453	0.4
Black box quantum neural network	0.9261	0.0577	0.8684	0.9
Large classical neural network	0.9908	0.4711	0.5197	0.46
Small classical neural network	0.9861	0.3718	0.6143	1

ratio because the fast gradient sign attack was produced with complete information about that classifier, and the perturbed images were not transferred to a different classifier. Both quantum neural networks had the highest maximum transferability ratios, followed by the small classical neural network, and then the large classical neural network.

4 Discussion

4.1 *Transferability*

The hypothesis that adversarially perturbed data designed to deceive the white box quantum neural network would also succeed in deceiving the other neural networks was supported. Therefore, there is transferability in adversarial examples. This is shown through the adversarial accuracies of all neural networks (except for the large classical one) being significantly lower than chance, and the low adversarial accuracy of the large classical neural network on the actual positives.

When evaluating the adversarial accuracy, it is important to determine whether the decrease in accuracy (as compared to the testing accuracy) is due to the success of the adversarial attack, or simply because the images have been modified and are thus inherently less recognizable. In the latter case, the modification of the images causes the classifier to extract less or even no information. Thus, at worst, the classifier's prediction is effectively random. If the adversarial accuracy of the classifier is significantly lower than chance, then the possibility that the decrease in accuracy is entirely due to the loss of information from the modification of the images can be ruled out, so it can be concluded that the adversarial attack played a role in decreasing that accuracy.

The adversarial attacks were effective against both quantum neural networks and the small classical neural network. Figure 1 shows that the fast gradient sign attack (on the white box quantum neural network) and the transfer attack (on the others)

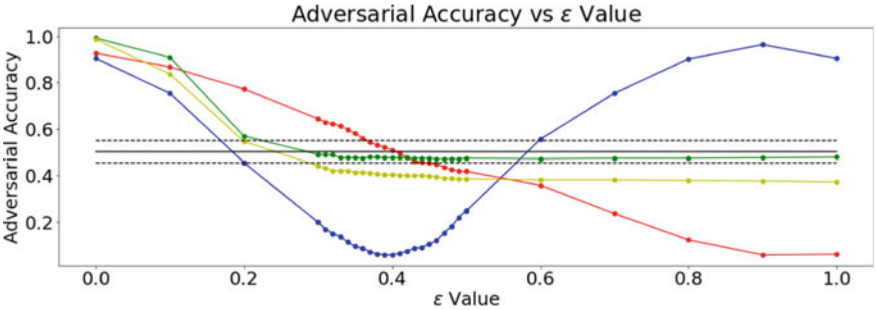


Fig. 1 This figure compares the adversarial accuracies (abbreviated as "accuracy") of all four models as ε changes. The accuracies of the white box quantum, black box quantum, large classical, and small classical neural networks are represented by the blue, red, green, and yellow curves, respectively. Dots represent actual data points, while the lines between are interpolations. The solid black line represents chance accuracy (0.50), while the dotted black lines above and below give a 95% confidence interval for a classifier with chance accuracy. All classifiers start with an accuracy above 0.90, and as ε increases from 0 to 0.4, their accuracies decrease. The white box quantum neural network reaches its minimum accuracy of 0.0577 when $\varepsilon = 0.4$, and both classical neural networks' accuracies start to settle around their final values. As ε increases beyond 0.4, the black box quantum neural network's accuracy continues to decrease, while the white box quantum neural network's accuracy increases. All models except for the large classical one have ε values for which their accuracy decreased to be significantly less than chance, demonstrating the effectiveness of the transfer attack and the fast gradient sign attack

reduced their minimum adversarial accuracy to a level that is significantly below chance. Therefore, the adversarial attacks succeeded against these models.

Against the large classical neural network, the transfer attack still succeeded, albeit to a lesser extent. Figure 1 shows that its adversarial accuracy never dips significantly below chance. However, that does not preclude the possibility that the transfer attack was still successful on a smaller portion of the images. Indeed, by examining Table 1, one can see that its adversarial accuracy is significantly ($p < 0.05$) below chance when predicting on the actual positives, even if the adversarial accuracy on the actual negatives was substantially higher. Therefore, the transfer attack succeeded in attacking the actual positive images, implying that the fast gradient sign attack still partially transferred to the large classical neural network.

4.2 Future Work

There are limitations to the scope to which the results may be applied. Future studies may use different attack methods, more computational resources, more varied types of models, and different datasets to assess the generality of the results.

5 Conclusion

The results support the hypothesis that the fast gradient sign attack, performed on the white box quantum neural network, can transfer to the other neural networks because the transfer attack decreased the accuracy to significantly below chance.

The transferability of the attack across models suggests that these neural networks, despite their differences (quantum vs classical, size, architecture), share a similarity in their weakness to the same adversarial attack. More generally, this suggests a common weakness that may exist in neural networks in general. Perhaps this is because the neural networks, in response to the same classification task, create similar decision boundaries with similar weaknesses.

As discussed in the section on future work, there are a few possible directions of future study. There are also a few potential applications of this work in addition to the ways previously described, such as the use of transferability to perform black box attacks, or to use it to construct better defenses against black box attacks. Furthermore, by better understanding the ways in which models can fail or be attacked, a more complete and comprehensive theory of quantum machine learning, especially quantum adversarial machine learning, can be developed, driving future innovations in machine learning.

References

1. Abadi M, Agarwal A, Barham P, Brevdo E, Chen Z, Citro C, Corrado GS, Davis A, Dean J, Devin M, Ghemawat S, Goodfellow I, Harp A, Irving G, Isard M, Jia Y, Jozefowicz R, Kaiser L, Kudlur M, Zheng X (2015) TensorFlow (Version 2.4.1) (Computer software). https://www.tensorflow.org
2. Adam SP, Alexandropoulos SAN, Pardalos PM, Vrahatis MN (2019) No free lunch theorem: a review. Approximation Optim, 57–82
3. Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, Biswas R, Boixo S, Brandao FGSL, Buell DA, Burkett B, Chen Y, Chen Z, Chiaro B, Collins R, Courtney W, Dunsworth A, Farhi E, Foxen B, Hoffmann M (2019) Quantum supremacy using a programmable superconducting processor. Nature 574(7779):505–510 https://doi.org/10.1038/s41586-019-1666-5
4. Broughton M, Verdon G, McCourt T, Martinez AJ, Yoo JH, Isakov SV, Massey P, Niu MY, Halavati R, Peters E, Leib M, Skolik A, Streif M, Von Dollen D, McClean JR, Boixo S, Bacon D, Ho AK, Neven H, Mohseni M (2020) TensorFlow quantum: a software framework for quantum machine learning. *arXiv*. Retrieved 11 Sept 2021, from https://arxiv.org/
5. Caswell TA, Droettboom M, Lee A, Sales de Andrade E, Hoffmann T, Hunter J, Klymak J, Firing E, Stansby D, Varoquaux N, Nielsen JH, Root B, May R, Elson P, Seppänen JK, Dale D, Lee J-J, McDougall D, Straw A, Ivanov P (2021) Matplotlib (Version 3.4.3) (Computer software). https
6. Cirq Developers (2021) Cirq (Version 0.12.0) (Computer software)
7. Ebrahimi J, Rao A, Lowd D, Dou D (2017) Hotflip: White-box adversarial examples for text classification. arXiv preprint arXiv:1712.06751
8. Glendinning I (2005) The bloch sphere. In: QIA meeting. Vienna
9. Goodfellow IJ, Shlens J, Szegedy C (2015) Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572

10. Harris CR, Millman KJ, van der Walt SJ, Gommers R, Vertanen P, Cournapeau D, Wieser E, Taylor J, Berg S, Smith NJ, Kern R, Picus M, Hoyer S, van Kerkwijk MH, Brett M, Haldane A, del Río JF, Wiebe M, Peterson P, Oliphant TE (2020) NumPy (Computer software). https://numpy.org
11. Huang L, Joseph AD, Nelson B, Rubinstein BI, Tygar JD (2011) Adversarial machine learning. In: Proceedings of the 4th ACM workshop on Security and artificial intelligence
12. LeCun Y, Cortes C, Burges C (2010) MNIST handwritten digit database . http://yann.lecun.com/exdb/mnist/
13. Lu S, Duan L-M, Deng D-L (2020) Quantum adversarial machine learning. Phys Rev Res 2(3):1–18. https://doi.org/10.1103/PhysRevResearch.2.033212
14. Pedregosa F, Varoquaux G, Gramfort A, Michel V, Thirion B, Grisel O, Blondel M, Prettenhofer P, Weiss R, Duborg V, Vanderplas J, Passos A, Cournapeau D, Brucher M, Perrot M, Duchesnay E (2011) Scikit-learn (Computer software). https://scikit-learn.org/stable/
15. Python Software Foundation (2021) Python (Version 3.7.11) (Computer language). https://www.python.org/
16. Rieffel E, Polak W (2000) An introduction to quantum computing for non-physicists. ACM Comput Surv (CSUR) 32(3):300–335
17. Ruder S (2016) An overview of gradient descent optimization algorithms. arXiv preprint arXiv:1609.04747
18. Schuld M, Sinayskiy I, Petruccione F (2015) An introduction to quantum machine learning. Contemp Phys 56(2):172–185
19. SymPy Development Team (2020) SymPy (Version 1.7.1) (Computer software). https://www.sympy.org/en/index.html
20. TensorFlow Developers (2021a) Calculate gradients. TensorFlow quantum. Retrieved 30 Aug 2021 from https://www.tensorflow.org/quantum/tutorials/gradients
21. TensorFlow Developers (2021b) MNIST classification. TensorFlow quantum. Retrieved 30 Aug 2021 from https://www.tensorflow.org/quantum/tutorials/mnist
22. TensorFlow Developers (2021c) Adversarial example using FGSM. TensorFlow. Retrieved 31 Aug 2021 from https://www.tensorflow.org/tutorials/generative/adversarial_fgsm

Conceptual Analysis and Design of Semantic Interoperability of Smart City Services

Sergei Kozhevnikov

Abstract Smart city projects now mainly focus on developing data management platforms. They help to store, process, visualize and provide data access for better services. The smart city knowledge management platform (KMP) is a more complex solution. Developing the city IT infrastructure based on KMP helps to achieve semantic interoperability between city actors and create a digital eco-system of smart services capable to negotiate, compete and cooperate. In this work, a detailed approach and step-by-step design and development instruction for KMP and semantic interoperability are presented.

Keywords Digital ecosystem · Ontology · Semantic interoperability · Smart city

1 Introduction

In developing and implementing smart city solutions, researchers face the problem of processing the vast amount of data of different origins (from sensors, GPS, video, mobile devices, IoT and others). The volume and value of the data and the number of sources of information grow tremendously. This data helps to provide better services for city residents and city managers and helps to have an accurate and clear view of the current state in various aspects. To gently it, cities usually create data management platforms (DMP) to process, store and give access for services under certain conditions [1].

The smart city knowledge management platform is a more complex solution. KMP should effectively use the existing data, transfer it to knowledge and keep the previously collected information safe. The main advantage of implementing KMP is a better data processing and the possibility of achieving semantic interoperability (SI) between various smart city systems and subsystems.

S. Kozhevnikov (✉)
CIIRC, Czech Technical University in Prague, Jugoslávských partyzánů, 1580/3 160 00 Prague 6, Czech Republic
e-mail: koz@kg.ru

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_72

2 Smart City as Digital Ecosystem

The smart city and Industry 4.0 concepts have much in common and can be presented as a set of specific applications for planning, control, analysis of all significant business (or living) processes working in a specific data and infrastructure environment.

Prominent manufacturers of industrial software systems have created complicated solutions with sets of functional modules, but usually face the problems of continuous and endless implementation. They are working on intelligent digitalization of business with no possibility to write all the requirements for the software solutions in advance. However, the conceptual, technological and architectural framework that defines significant aspects of the development should be chosen at the very beginning.

By the end of the 2010s, the ERP concept lost flexibility concerning new business processes [2]. It happened because enterprises (as smart cities now) are constantly changing and growing in complexity. The second factor is the unavailability to create one centralized monolithic system based on a single universal data repository. At the same time, the smart city developers have faced the problem of integration of submodules in conventionally monolithic systems and integration with external systems from other manufacturers [3].

In this regard, in recent years, a more pragmatic approach called "Postmodern ERP" has become widespread, within which consumers could choose the most successful modules from different providers. The primary condition is that all the systems and subsystems should work together and give a positive synergetic effect [4]. This task is decisive for Industry 4.0 and smart city concepts, which is not fully solved yet.

The promising way of creating smart cities is the collaborative development of an open-source digital platform performed by communities of city actors but based on the predefined standards of data/knowledge structures and interaction protocols of elements of the system [5]. It appears as a network structure built on the principles of self-organization, competition and cooperation, focused on business tasks.

On the general level, the open-source digital platform ensures the automation of routine business processes by supporting the operation of various business entities of the smart city. On the local level, services are provided by local companies. Each business entity on every level can support an event-driven operation scheme (triggered by foreign events and generated its events), interact with other modules, support business processes.

This will lead to the smart city performing as a digital ecosystem based on the postmodern ERP principles (Fig. 1).

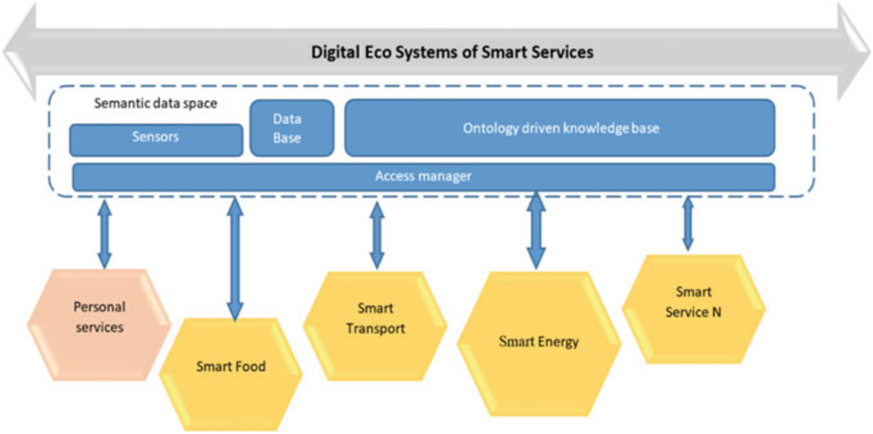


Fig. 1 Digital eco-system architecture

3 State of the Art

Every city is a complex system of social and socio-technical networks, a combination of technical systems and human organizations. Therefore, SC is considered as a complex adaptive network-centric system of systems with a tremendous amount of actors and links between them. To achieve better interaction, it should be developed based on a common ontology-driven knowledge base [5].

One of the problems of managing ontologies is the high rate of change of underlying data. Intelligent ontologies of cities are very dynamic, and data changes must be timely reflected [6]. The main problem is that ontology-driven knowledge bases are updated manually when a new element is added to the ecosystem or when a new agent, not defined by the system, wants to use services or data [7]. Despite that, this technology is widely investigated and evaluated in practical application in smart city projects.

VITAL (European project) is working on modelling IoT data streams generated by different SC devices. The task is to overcome the problem of heterogeneity [8]. VITAL can reuse a highly detailed set of ontologies describing many aspects of devices with the support of ontology.

The km4City ontology reuses the basic vocabularies of several ontology standards [9]. The model's description shows that the small size of the km4City ontology results in more straightforward possibilities to reuse it in innovative city applications. However, based on further publications, the industrial implementation of km4City ontology is not achieved.

SOFIA project presents a platform developed in Spain to collect the data from various sources SC elements [10]. It shows the possibility to operate among different urban systems. But also it proves the concept of predefined templates that have been already implemented into the ontology.

The general smart city knowledge base can be developed as a set of ontologies of other domains [11]. Authors try to minimize ontology commitments, avoid developing large monolithic ontologies and use small and generic ontology snippets, which capture key on the one side and reusable on the other side knowledge.

Attempts to achieve semantic interoperability in the smart city concept are made by Concoli et al. [5]. The research aspects of sharing heterogeneous data between various e-services on the example of Catania City based on the Linked Open Data technology are described. But no results of practical implementation are presented.

It is interesting to mention the idea of generally accepted semantics for intelligent devices and use of reference ontology as an interaction language [12]. Use cases include several areas, but project more focuses on increasing production process flexibility.

Trained neural networks can be integrated into multi-agent systems used by agents to interpret concepts of a given ontology and provide an exact precise meaning to a message sent by agents to each other [13]. Deep learning with multi-agent technology can be used as a solution to define new meanings in the ontology.

The knowledge management software is crucial to develop a fundamentally new open digital smart city platform that supports models and methods of collective, coordinated decision-making and implemented in an expandable network of interacting intelligent solutions. It helps to solve the storage of dynamically expandable sets of data, data transfer between services, standards for data exchange, negotiation protocols between systems for consensual decisions, information security and safety [14].

Basic principles to design and develop an open-source digital smart city platform with semantic interoperability of smart services:

1. City can be “smart” only by enforcing cooperation/competition of services.
2. Extracting knowledge from current data is not enough because the current way of running services is, as a rule, inefficient and usually needs to be changed entirely.
3. Collecting data from existing services is crucial but not enough to scale and scoop future solutions. The knowledge base should be expandable.
4. Cooperation of services in the smart city concept 5.0 should be made concerning semantic interoperability of services.
5. The SC knowledge base can be designed as combinations of different small ontologies of various problem domains (the generic ontology, specific ontologies).

It was shown in [15] that the smart city should be a network-centric system of systems, based on knowledge bases and ontologies (as the most promising method of ensuring interoperability of actors).

We have estimated four different approaches in the case of interoperability that interacting systems use to share and operate on data. In our research, we take into account only semantic interoperability task and consider all other levels (technical, organizational, syntax) out of scope.

4 Conceptual Design of the Semantic Interoperability

4.1 Semantic Interoperability Definition

Most of the city services developed and implemented are functionally and semantically separated. Collaboration between them is rigid and predefined. However, users often choose the best services, even from different providers or digital ecosystems.

The complexity of the systems is continually enhanced, elevating risk and maintenance costs and delivery times. To force two systems to work together, it is needed to use common databases, manually create and manage knowledge bases, or use a service-oriented architecture that is limited in scale. Integration through knowledge bases and semantic description is very perspective but complicated and primarily manual work.

Semantic description (SD) technology does not provide semantic interoperability by design and does not solve all the knowledge-gathering, management and sharing tasks. The SD of different problem domains should always be processed according to a specific predefined procedure.

In terms of integration of services, the SC developers usually make a step towards creating city databases and managing access rights [1]. Less steps towards semantic interoperability are made. Every service joining the digital smart city ecosystem must know specific information about it and other services. It is crucially valuable that systems, devices and components can interact and understand each other to some extent (within the context of their intended collaboration) [15, 16]. For that, systems should understand their role in the collaboration: what functions they have and provide, what services they offer to the user, what kind of limitations they have.

The updated with [17] definition of semantic interoperability:

- is working with the meanings of data;
- helps systems to find the consensus of meaning;
- ensures that the meaning is defined the same way for all actors and mutually agreed by them;
- enables different stakeholders to access and understand data unambiguously.

4.2 Ontology for Semantic Interoperability

Semantic interoperability is used for managing and exchanging knowledge between systems and is based on finding related terminology concepts.

Choosing the ontology as an instrument of semantic data description will make it interoperable for users and services that share one same ontology. Ontologies are used for semantic interoperability for automated reasoning and advanced services to smart applications such as conceptual search, semantic search (non-keyword based), joint work with software agents, decision support, natural language understanding, knowledge management.

For most efficient use, different services should have a common agreement on ontological definitions. Most of the existing ontologies and semantic description frameworks in the smart city concepts are explained in the context of different problem domains and are currently at an early stage. A common semantic annotation framework and ontology definitions of basic concepts were the key issues to achieve global semantic interoperability.

Designing, developing and sharing ontologies and contributing to description and annotation frameworks supporting legacy applications are reasonable steps in achieving interoperability on a large interdisciplinary scale. Different solutions, such as ontology mapping and matching (i.e. manual, semi-automated, or automated), can help link the resources described using different semantic annotation models. The ontology designers can also reference common ontologies and provide links to other upper-level ontologies to support interoperability between different semantic descriptions.

We use a combination of these principles. It can be used horizontally among smart city services for better organization or vertically with the basic smart city knowledge in updating the basic city ontology.

4.3 Main Steps in Design of SI

The main topics to be solved for the semantic interoperability of services can be distinguished as: ecosystem rules, knowledge base of the ecosystem, functionality of smart services, mechanism of interaction.

As the basic steps in designing the open-source digital platform for smart city services it is important to check:

- All the elements and smart services use one language and understand each other.
- New services are presented to each other, explaining their basic functionality.
- Need to update the knowledge base of the platform if new valuable information arrives with new service.
- Different services should start to negotiate between each other and customers offering new products.

To solve this task, a conceptual approach for creating an open-source digital platform is proposed. It is based on multilevel ontology architecture and multi-agent matchers for mapping ontologies.

In the design of the smart city SI, we should start from the particular steps of analysis. First of all, we need to analyse the complexity of data used by the smart city and assess different levels of interoperability:

1. The quantitative data indicators: sources of data, growing rate, number of diversity and heterogeneous formats.
2. Qualitative data indicators: processing speed, diversity of data in different problem domains.

3. Processing instruments: diversity of approaches, methods and instruments, diversity of data models

As the second step, we need to assess the general requirements for the smart city knowledge base in case of semantic interoperability. General requirements are: requirements for data representation, validation data requirements, access rights requirements, requirements for data taxonomy, privacy and security requirements.

To design, as the next step, the general smart city knowledge base platform it is important to define several aspects to be considered. Most important among them:

1. In semantic data modelling:
    - the semantic representation of data to form one common understanding across services.
2. Semantic integration and sharing:
    - the matching and mapping mechanism to support dynamic integration and sharing.
3. Semantic description of data:
    - a semantic description mechanism to support the annotation of data coming from heterogeneous sources.
4. Ecosystem rules for knowledge management:
    - Instruments to work with the data including access rights, storage options.
5. Semantic Ontology matching and mapping:
    - Instruments to collect and understand of heterogeneous semantics from different systems.
    - Matching and mapping service to parse the new knowledge arriving and align it with existing knowledge to support semantic interoperability.
6. Representation of knowledge:
    - Representation of the knowledge in the way that supports reasoning and validation of the information.
    - Possibility to provide the partial view of the whole knowledge base.

This project proposes architecture design of a general ontology model of the city (as metaontology) and its services (smart service ontologies, onto-models) stored in the KMP. This will allow various players to create or choose various services for themselves and further refine their ontology. It is assumed that companies operating based on the created eco-system of city services will offer and sell their generalized and typed onto-models to other participants in future. For this, it is necessary to create basic principles and concepts based on which the city ontology will be created.

In addition, the SC KMP may include various types of normative and reference information most commonly used by various companies in the subject area and other information necessary for building and synchronizing plans.

4.4 Architecture of the Software Solution

The smart city ontology (SCO) as the primary instrument of KMP was created as a formalized model of domain knowledge, in fact, an "explanatory dictionary" for intelligent decision-making systems. SCO was created as a semantic network of classes of concepts and relations of the smart city.

SCO consists of three levels of ontologies:

1. City metaontology. It is a set of basic concepts and rules that are predefined and cannot be changed.
2. Basic ontology of the city. The second level is created based on the metaontology concepts and rules, but can be changed in the operation process.
3. Private ontologies of smart services (companies, people and other players). The dynamic part can be added when the new actors want to join the smart city ecosystem.

It is essential to mention that private ontology if the problem domain is new, can add new knowledge and change the basic ontology of the city.

In the case of the new smart service that intends to join the smart city ecosystem, we use two types of multi-agent matchers to integrate the new ontology into the existing one. The process runs as follows:

1. The formal matching process. Check if the existing ontology matches the new one.

   - Check the consistency of syntax (we speak the same language).
   - Check the correspondence between the base classes of metaontology and new ontologies (we use a basic set of words).
   - Check the conformity of the ontology (check the entire vocabulary).
   - Show non-alignment (discrepancies) between ontologies.
   - Offer to make changes in the new ontology so it will fit (if needed).

2. The semantic matcher tries to understand the meaning of the new service. On this level, we need to answer the question: Who are you? What tasks do you solve? Where do you store the knowledge? How to use you?

   - Propose to make changes and add new knowledge to the basic ontology (to expand the base vocabulary)

     The agent-based ontology matchers should coordinate the ontologies on two levels:
   - formal—matching the new ontologies.

- semantic level—looking at the new ways of cooperative work between services.

When the new service arrives to the ecosystem with its own ontology KMP checks the new participant in case of the knowledge can be used. The new participant is interested in providing as much information as possible.

The formal matcher checks the new ontology if it can be used ("talking on the same language step"). On the next stage, the semantic matcher tries to understand the meaning of the new service ("how we can be helpful for you"). The new ontology can be written from different perspectives: functionality, business process, technological process, organization structure. The more information is provided the better cases semantic matcher can later find for the new service.

Experiments performed with ontologies matching process show the main conflicts that can be identified:

- Name conflicts ("citizen" or "resident").
- Isomorphism conflicts (different composition of attributes).
- Different details in problem domain.
- Different structures of entities.
- Data presentation.
- Measurement units (metric, non-metric).

Developing the knowledge management platform to achieve semantic interoperability, several issues should be considered:

1. Due to the heterogeneity of existing ontological sources and the variety of applications in which matchers should be used, it is clear that general ontology matching algorithms are unable to serve each type of ontology, provide the desired inference and cope with excessive requirements for the application.
2. We recognized the need for a strategy that seeks to optimize the matching process while at the same time being aware of the inherent dependencies between current ontologies.
3. To solve the problems of heterogeneity and plurality of existing ontologies, we have implemented the metaontology framework and standard as a set of rules and basic concepts to be used by the new services of the ecosystem.
4. Systems complement each other's ontologies.
5. The possibility of various technology stacks of smart city services forced to choose the OWL ontology standard.

Conflicts can be avoided if the basic principles and rules of the metaontology will be used by each new service in the smart city digital ecosystem. It will not limit the functionality but open the way for better semantic cooperation.

5 Conclusion

There are two main trends in developing smart city solutions: the transition from centralized software products to a modular systems and digital ecosystems. Considering the principles of postmodern ERP the smart city as an ecosystem of integrated network of smart service can be developed. New modules should be easily integrated into the software environment on the "plug-and-play" principle and be semantically connected. This will help to achieve the new commercial advantages and implement the modern economy approach—distributed work on distributed tasks.

Semantic interoperability can differ—from exchanging simple data package to cooperative decision-making in decentralized systems, finding different hidden logic and variants for cooperation. For the smart city concept, we focus on the cases when the new business process of new smart services can find gentle cooperation opportunities with other organizations and services through OSDP platform.

The result of the project will lead to the new standards of ontological representation, services negotiation protocols and standards for smart city metaontology.

Acknowledgements This work was supported by the European Regional Development Fund under the project AI & Reasoning (reg. no. CZ.02.1.01/0.0/0.0/15_003/0000466).

References

1. https://golemio.cz/cs/o-projektu
2. Katuu S (2020) Enterprise resource planning: past, present, and future. New Rev Inf Netw 25(1):37–46. https://doi.org/10.1080/13614576.2020.1742770
3. Kupriyanovsky VP, Yartsev DI, Kharitonov AA, Utkin NA, Nikolaev DE, Drozhzhinov VI, Namiot DE, Volokitin YI (2017) Semantics, metadata and ontologies in applications for smart city—new bsi standards. Int J Open Inf Technol 6
4. https://spb.1cbit.ru/company/news-spb/369052/#top1
5. Consoli S et al (2017) Producing linked data for smart cities: the case of Catania. Big Data Res 7:1–15
6. Hernandez-Mendez A, Faber A, Bondel G, Matthes F (2018) Towards an ontology-based information system for smart city ecosystems. In: Proceedings of the 24th Americas conference on information systems, New Orleans
7. Callaghan V, Intelligent association exploration and exploitation of fuzzy agents in ambient intelligent environments
8. Bellini P, Benigni M, Billero R, Nesi P, Rauch N (2014) Km4city ontology building vs data harvesting and cleaning for smart-city services. J Vis Lang Comput 25(6). https://doi.org/10.1016/j.jvlc.2014.10.023
9. European Commission. New ontology specification for smart cities, industry 4.0 and smart agriculture. https://digital-strategy.ec.europa.eu/news/etsi-releases-three-new-saref-ontology-specifications-smart-cities-industry-40-and-smart (11 Sept 2020)
10. Otero-Cerdeira L, Rodríguez-Martínez FJ, Gómez-Rodríguez A (2014) Definition of an ontology matching algorithm for context integration in smart cities. Sensors (Switzerland) 14:23581–23619

11. Kazmi A, Jan Z, Zappa A, Serrano M (2016) Overcoming the heterogeneity in the internet of things for smart cities. In: International workshop on interoperability and open-source solutions. Springer
12. Espinoza-Arias P, Poveda-Villalón M, García-Castro R, Corcho O (2019) Ontological representation of smart city data: from devices to cities. Appl Sci 9(1):32. https://doi.org/10.3390/app9010032
13. Augusto JC, Nakashima H, Aghajan H (2010) Ambient intelligence and smart environments: a state of the art. In: Nakashima H, Aghajan H, Augusto JC (eds) Handbook of ambient intelligence and smart environments. Springer, Boston. https://doi.org/10.1007/978-0-387-93808-0_1
14. Přibyl P, Přibyl O, Svítek M, Janota A (2020) Smart city design based on an ontological knowledge system. In: Research and the future of telematics. Communications in computer and information science, vol 1289. Basel: Springer Nature Switzerland AG, pp 152–164. ISSN 1865-0929. ISBN 978-3-030-59269-1
15. Svítek M, Skobelev P, Kozhevnikov S (2020) Smart city 5.0 as an urban ecosystem of smart services. In: Borangiu T, Trentesaux D, Leitão P, Giret Boggino A, Botti V (eds) Service oriented, holonic and multi-agent manufacturing systems for industry of the future. SOHOMA 2019. Studies in Computational Intelligence, vol 853. Springer, Cham
16. Svitek M (2011) Applying wave probabilistic functions for dynamic system modeling. IEEE Trans Syst Man Cybernet Part C-Appl Rev 41(5):674–681
17. El Abid Amrani N, Youssfi M, Abra OEK (2018) Semantic interoperability between heterogeneous multi-agent systems based on deep learning. In: International conference multimedia computer system –proceedings, 1–6 May 2018

Construction and Analysis of Kepler's Cosmographic Mystery, for Learning the Platonic Solids Using Mathematica

Felícita M. Velásquez-Fernández, Judith K. Jiménez-Vilcherrez, Carlos E. Arellano-Ramírez, Robert Ipanaqué-Chero, and Ricardo Velezmoro-León

Abstract This research work revolves around the need to learn regular polyhedral constructions and find the relationships that exist with the spheres that inscribe them in the structure of Kepler's Cosmographic Mystery. We often do not realize that polyhedra are present in almost everything around us, and that throughout history, man has been fascinated by Platonic solids. At present, students live in reverse in the massive use of electronic equipment in their learning, as well as software and applications. Given the high demand for the acquisition of digital skills worldwide, students can be motivated to strengthen their learning of mathematics and acquire programming skills by observing, analyzing and arguing a programming strategy to design the Cosmographic Mystery of Kepler, also the existing relationships in the structure under study. Therefore, through this work, it is intended to provide the teacher with resources and programming skills for the teaching of regular polyhedra. Mathematica software has been considered for its high programming and display quality. In addition, the Wolfram programming language is accessible through the Raspberry computer. The objective of the research work is to provide a working methodology for the study of regular polyhedra and acquire programming skills. Also, strengthen their observation and analysis skills from their models for the design of Platonic polyhedra through the programming language, allowing students to explore 3D spaces.

F. M. Velásquez-Fernández (✉)
Universidad César Vallejo, Av. Chulucanas s/n-Distrito 26 de Octubre, Piura, Peru
e-mail: fmvelasquezf@ucvvirtual.edu.pe

J. K. Jiménez-Vilcherrez
Universidad Tecnológica del Perú, Av. Vice Cdra 1, Piura, Peru
e-mail: C19863@utp.edu.pe

C. E. Arellano-Ramírez · R. Ipanaqué-Chero · R. Velezmoro-León
Universidad Nacional de Piura, Urb. Miraflores s/n Castilla, Piura, Peru
e-mail: carellanor@unp.edu.pe

R. Ipanaqué-Chero
e-mail: ripanaquec@unp.edu.pe

R. Velezmoro-León
e-mail: rvelezmorol@unp.edu.pe

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_73

Keywords Mathematica · Cosmographic · Kepler · Construction · Regular polyhedra

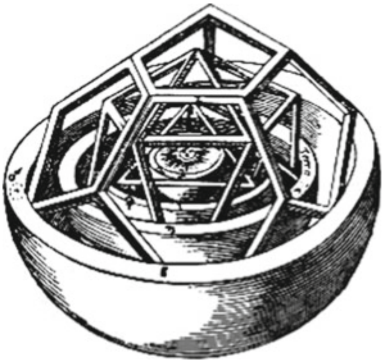
1 Introduction

Johannes Kepler was a mathematician fascinated by Euclid's geometry. He saw God as the Perfect Geometer, creator of the universe. In his attempt to give an explanation to the geometry of the universe, he associated the five Platonic solids with the planetary orbits known in his time. I nest them one inside another, and he presented it in 1635 his astronomy book titled Mysterium Cosmographicum where he tells us [1].

"The earth is the circle that is the measure of everything. Circle it a dodecahedron. The circle that inscribes it will be Mars. It circumscribes Mars with a tetrahedron. The circle that includes that will be Jupiter. Circle Jupiter with a cube. The circle that comprises this will be Saturn. Now inscribe an icosahedron in the earth. The circle inscribed in this will be Venus. Inscribe an octahedron on Venus. The circle inscribed on it will be Mercury. You are right about the number of planets." (See Fig. 1).

Now, considering the historical richness from the geometric point of view of Kepler's scientific activity, when trying to explain the cosmos through Platonic polyhedra, interest arises from the construction of Kepler's Cosmographic Mystery using Mathematica software, with the aim that it allows students to interpret, understand and appreciate the geometric beauty that the scientist described. From this model, students develop spatial thinking and strengthen their logical as well as deductive thinking. Students will make use of the properties, relationships between three-dimensional and two-dimensional objects. Through observation, look for interrelationships that allow the construction of each of the Platonic polyhedra and thus add them to each other inscribed in concentric spheres.

Fig. 1 Kepler's cosmographic mystery



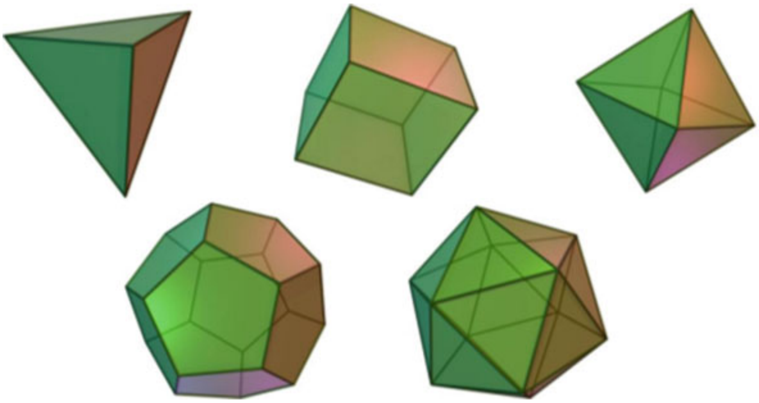


Fig. 2 Platonic polyhedra: tetrahedron, cube, octahedron, dodecahedron and icosahedron

Whereas, in regular basic education, emphasis is placed on process and activity, as well as knowledge. Mathematical competence is directed at the ability to use mathematical modes of thought and representation.

There are various mathematical softwares that favor the integration of visualization processes, favoring the study and properties of three-dimensional objects. Among the different softwares, the Mathematica Software was chosen for its interface and its high level of programming and 3D visualization; it also has the goodness of being compatible with the Raspberry computer, making it accessible to students.

From these approaches, the research question arises: Does Software Mathematica management makes it possible to learn Platonic solids by representing Kepler's universe and analyzing the metric relationships that exist between planetary spherical orbits and polyhedra?

The structure of this document is as follows: Sect. 2 gives some definitions and characteristics of the Platonic solids. It also explains the structure of Kepler's Cosmos. Sect. 3 talks about the analysis for the construction of Platonic solids. Sect. 4 describes the construction of Kepler's Cosmos. The document closes with the main conclusions and some additional observations in Sect. 5.

2 Mathematical Preliminaries

By definition, a Platonic solid is said to be a regular polyhedron. The regularity in space is understood that the faces of the regular polyhedron are equal to each other and whose vertices are uniform; in addition, convexity is required [3].

Platonic polyhedra are the tetrahedron, the cube (or hexahedron), the octahedron, the dodecahedron and the icosahedron, see Fig. 2:

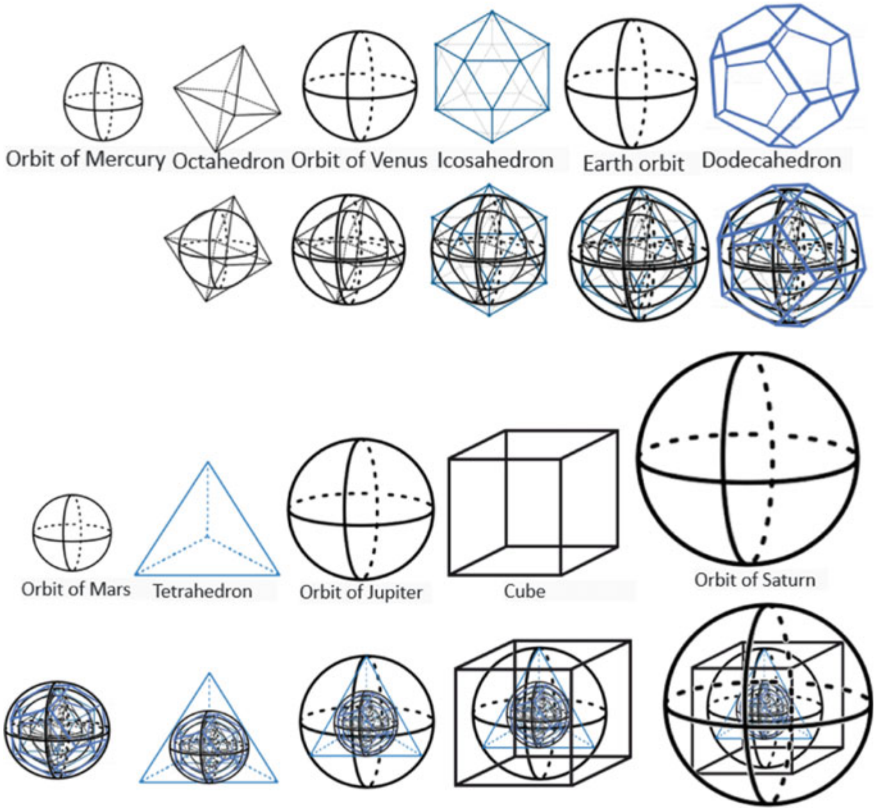


Fig. 3 Kepler's mystery of the cosmos building structure

Regarding Kepler's Cosmographic World, due to his eagerness to find an explanation of the planetary movements through the relationships between the orbits of the planets, he tried to represent them as the quotient of the size of the spheres in which he inscribed the perfect polyhedra.

The structure of the Cosmographic Mystery that Kepler considered is the following (Fig. 3):

3 Construction of the Platonic Solids

Geometry studies the shapes of figures and geometric bodies; among its objects of study are polyhedra [4].

Geometry studies the shapes of figures and geometric bodies; among its objects of study are polyhedra. It is important that students learn polyhedra due to the need for human beings to define their surroundings, their shapes, dimensions and the place they occupy.

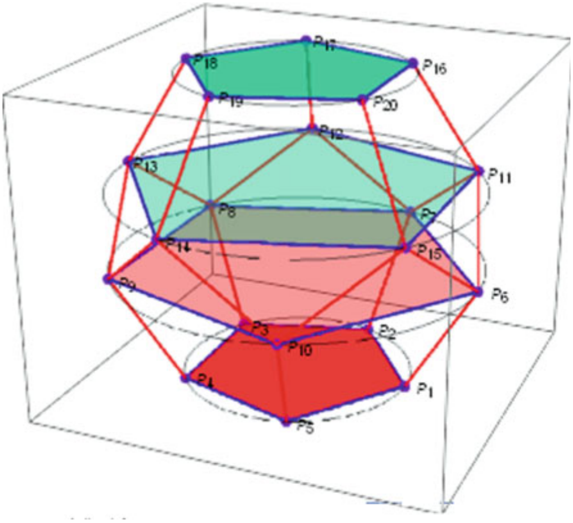


Fig. 4 Analysis for the construction of dodecahedron using Mathematica

Geometry studies the shapes of figures and geometric bodies, among its objects of study are polyhedra. It is important that students learn polyhedra due to the need for human beings to define their surroundings, their shapes, dimensions and the place they occupy.

At the world level, the curricular guidelines in basic education coincide in the importance of geometry as a tool to interpret the world that surrounds us, it also allows us to develop spatial, analytical and logical thinking, strengthening the argumentative processes regarding the characteristics and properties of the mathematical objects that are displayed.

Without a doubt, through the construction of Platonic polyhedra, students will develop spatial thinking because it encourages reasoning to seek a construction strategy through observation for later programming in the Mathematica scientific software.

Next, we will describe the construction reasoning for each of the Platonic polyhedra.

For the construction of these polyhedra, we will use analogous procedures reflected in a previous publication on the construction of the dodecahedron [5].

In the dodecahedron, it is visualized that its vertices also belong to 4 regular polygons parallel to one of the faces that we assume as a base (Fig. 4).

Using the same reasoning, the other regular polyhedra were built, that is, generating them from a special characteristic such as the one observed in the dodecahedron. The commands used to build the Platonic polyhedra are:

OctahedronCER[R], IcosahedronCER[R], DodecahedronCER[R], Tetrahedron CER[R], CubeCER[R]

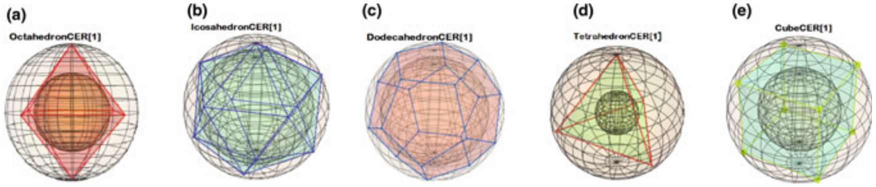


Fig. 5 **a** Octahedron circumscribed to sphere of radius *R*. **b** Icosahedron circumscribed to sphere of radius *R*. **c** Dodecahedron circumscribed to sphere of radius *R*. **d** Tetrahedron circumscribed to sphere of radius *R*. **e** Cube circumscribed to sphere of radius *R*

whose input is the radius "*R*" of the sphere inscribed in the polyhedron; its output is the visualization of its respective Platonic polyhedron, which in turn is inscribed in a sphere of radius "*r*". It also shows us the list of the vertices of their respective regular polyhedron.

3.1 Visualization of the Octahedron, Icosahedron, Dodecahedron, Tetrahedron and Cube

See Fig. 5

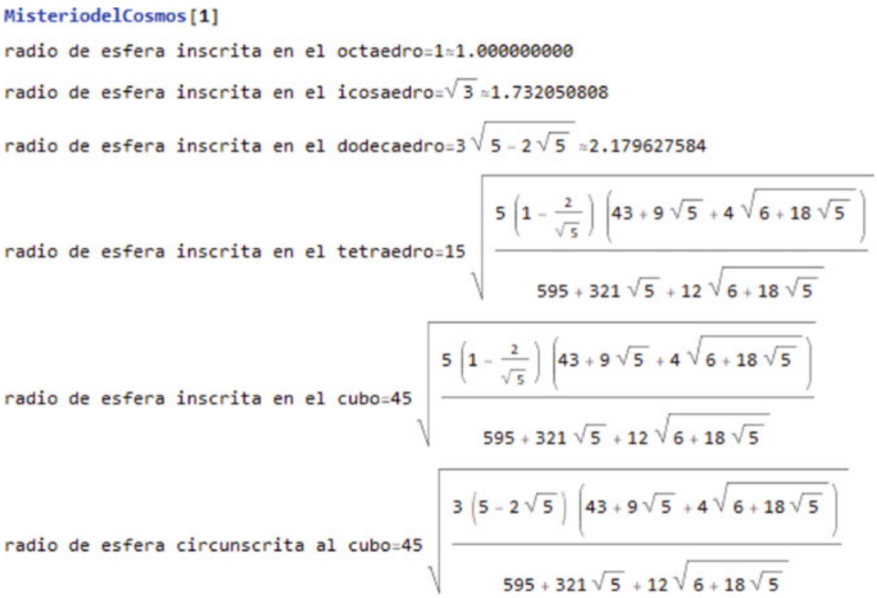
4 Kepler's Cosmographic Mystery Construction

The command $MisteriodelCosmos[r]$, whose input is the radius of the sphere that represents the orbit of Mercury, allows us to visualize Kepler's Cosmographic Mystery and the radii of each of the orbits as well as the vertices of each of the polyhedra Platonists.

In this case, we will generate Kepler's Mystery of the Cosmos from radius 1 of the spherical orbit of Mercury (Fig. 6).

5 Conclusions

The reasoning for the construction of each of the polyhedra can be generated from one of the regular faces, which is assumed to be the support base in the XY plane. Using certain characteristics, the student may be able to observe through the models the presence of polygons parallel to the base and whose vertices belong to the polyhedron. Taking advantage of this characteristic and certain properties, the student will be able to program or understand the programming language of the commands. Through the



MisteriodelCosmos[1]

radio de esfera inscrita en el octaedro=1≈1.000000000

radio de esfera inscrita en el icosaedro=$\sqrt{3}\approx 1.732050808$

radio de esfera inscrita en el dodecaedro=$3\sqrt{5-2\sqrt{5}}\approx 2.179627584$

radio de esfera inscrita en el tetraedro=$15\sqrt{\dfrac{5\left(1-\frac{2}{\sqrt{5}}\right)\left(43+9\sqrt{5}+4\sqrt{6+18\sqrt{5}}\right)}{595+321\sqrt{5}+12\sqrt{6+18\sqrt{5}}}}$

radio de esfera inscrita en el cubo=$45\sqrt{\dfrac{5\left(1-\frac{2}{\sqrt{5}}\right)\left(43+9\sqrt{5}+4\sqrt{6+18\sqrt{5}}\right)}{595+321\sqrt{5}+12\sqrt{6+18\sqrt{5}}}}$

radio de esfera circunscrita al cubo=$45\sqrt{\dfrac{3\left(5-2\sqrt{5}\right)\left(43+9\sqrt{5}+4\sqrt{6+18\sqrt{5}}\right)}{595+321\sqrt{5}+12\sqrt{6+18\sqrt{5}}}}$

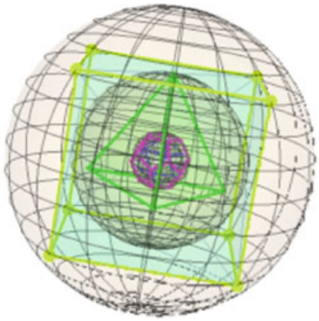


Fig. 6 Kepler's cosmographic mystery, constructed from the sphere radius of radius R that represents the orbit of mercury

commands, we will visualize the polyhedra with their vertices in 3D, as well as Kepler's Cosmographic Mystery with the list of the radii of the spherical orbits and the vertices of the polyhedra.

The radius that inscribes and circumscribes each of the polyhedra whose centroid is (0,0,0) and its vertices was calculated. But it was generalized, for them it was necessary to find the factor that we had to multiply the set of vertices according to the position established by Kepler, from the radius of the sphere that represents the orbit of Mercury. The factors found are: Factor that multiplies the vertices of the octahedron:

$$\frac{R}{\frac{1}{\sqrt{3}}}$$

Factor that multiplies the vertices of the icosahedron:

$$\frac{R}{\sqrt{\frac{\sqrt{5}}{6}+\frac{5}{12}}}\frac{1}{\frac{1}{\sqrt{3}}}$$

Factor that multiplies the vertices of the dodecahedron:

$$\frac{R}{\sqrt{\left(\frac{1}{2}+\frac{1}{\sqrt{5}}\right)^2+\frac{\left(3\sqrt{18\sqrt{5}+6}+4\right)^2}{1600}+\frac{1}{4}+\frac{1}{2\sqrt{5}}}}\frac{\sqrt{5}}{2\sqrt{\frac{\sqrt{5}}{6}+\frac{5}{12}}}\frac{1}{\frac{1}{\sqrt{3}}}$$

Factor that multiplies the vertices of the tetrahedron:

$$\frac{R}{\frac{1}{2\sqrt{2}}}\frac{\sqrt{\frac{1}{4}\left(\frac{1}{2}\sqrt{\frac{3}{2}\left(3\sqrt{5}+1\right)}+1\right)^2+1}}{\sqrt{\left(\frac{1}{2}+\frac{1}{\sqrt{5}}\right)^2+\frac{\left(3\sqrt{18\sqrt{5}+6}+4\right)^2}{1600}+\frac{1}{4}+\frac{1}{2\sqrt{5}}}}\frac{\sqrt{5}}{2\sqrt{\frac{\sqrt{5}}{6}+\frac{5}{12}}}\frac{1}{\frac{1}{\sqrt{3}}}$$

Factor that multiplies the vertices of the cube:

$$\frac{R}{\frac{1}{\sqrt{2}}}\frac{3}{\frac{2\sqrt{2}}{2\sqrt{2}}}\frac{\sqrt{\frac{1}{4}\left(\frac{1}{2}\sqrt{\frac{3}{2}\left(3\sqrt{5}+1\right)}+1\right)^2+1}}{\sqrt{\left(\frac{1}{2}+\frac{1}{\sqrt{5}}\right)^2+\frac{\left(3\sqrt{18\sqrt{5}+6}+4\right)^2}{1600}+\frac{1}{4}+\frac{1}{2\sqrt{5}}}}\frac{\sqrt{5}}{2\sqrt{\frac{\sqrt{5}}{6}+\frac{5}{12}}}\frac{1}{\frac{1}{\sqrt{3}}}$$

It can be verified that these factors that multiply the vertices coincide as the radius of the sphere that inscribes each of the polyhedra.

Students will be able to observe, understand, analyze and argue their reasoning for the construction of regular polyhedra and Kepler's Cosmographic Mystery using the Mathematica programming language. In the future, it is suggested to study the harmonic proportion that the beauty of the geometric structure of Kepler's Cosmographic Mystery exists. The implementation of TICs in the learning of Platonic solids allows the student to appropriate the new knowledge, by constructing the Platonic solids using their knowledge of plane geometry. The visualization provided by the dynamic Mathematica program allows the student to manipulate mathematical objects and can determine the characteristics and properties of Platonic polyhedra [6].

References

1. Coronado G (1995) Kepler y el misterio del Cosmos. Rev. Filosofía. Costa Rica XXXIII(81):137–142. http://www.inif.ucr.ac.cr/recursos/docs/Revista%20de%20Filosof%C3%ADa%20UCR/Vol.XXXIII/
2. Mayorga M, Gallardo M, Jimeno M (2015) Diagnostic evaluation in Andalusia: a study of the assessments in the skills in mathematics. Aula Abierta vol 43. https://doi.org/10.1016/j.aula.2014.07.001
3. Cromwell P (2004) Polyedra. University Press, Cambridge
4. Godino J, Batanero C (2011) Formacin de profesores de matemÃąticas basada en la reflexiÃşn guiada sobre la prÃctica. En L. Serrano (ed), Tendencias actuales de la investigaciÃşn en educaciÃn estocÃąstica, pp 9-33. MÃąlaga: Universidad de Granada. http://www.ugr.es/~batanero/pages/ARTICULOS/libroluis.pdf#page=9
5. Velezmoro León R, Velásquez Fernández M, Jiménez Gomez J (2020) Construction of the regular dodecahedron with the MATHEMATICA. In: Gervasi O et al (eds) Computational science and its applications âĂŞ ICCSA 2020. ICCSA 2020. Lecture notes in computer science, vol 12249. Springer, Cham. https://doi.org/10.1007/978-3-030-58799-4_27
6. GÃven B, Kosa T (2008) The effect of dynamic geometry software on student mathematics teachersâĂŹspatial visualization skills. Turk Online J Educ Technol 7(4):100–107https://files.eric.ed.gov/fulltext/EJ1102930.pdf

Meaningful Learning of Regular Basic Education Students in the Construction of Polyhedra from the Cube in a Graphical 3D Geometry Environment

Felícita M. Velásquez-Fernández, Judith K. Jiménez-Vilcherrez, Daniel A. Flores-Córdova, Robert Ipanaqué-Chero, and Ricardo Velezmoro-León

Abstract This research paper revolves around the need to learn polyhedral constructions. Students often do not realize that polyhedra are present in almost everything around them: microorganisms, minerals, architectural constructions and virtual reality objects. Currently, there is an accelerated process in the acquisition of digital skills worldwide, which can motivate and strengthen the meaningful learning of mathematics. For this reason, it is important that the teacher manages technological resources for the teaching of mathematics and thus awaken the student's interest in learning. We consider GeoGebra free software as an excellent tool to develop digital and spatial skills in the student for the understanding and construction of polyhedra from previous geometric concepts. The objective of the research work is to propose a work methodology for the construction of new polyhedra from the regular hexahedron using GeoGebra, allowing students to explore 3D spaces.

Keywords GeoGebra · Learning · Construction · Polyhedra · Cube

F. M. Velásquez-Fernández (✉)
Universidad César Vallejo, Av. Chulucanas s/n-Distrito 26 de Octubre, Piura, Peru
e-mail: fmvelasquezf@ucvvirtual.edu.pe

J. K. Jiménez-Vilcherrez
Universidad Tecnológica del Perú, Av. Vice Cdra 1, Piura, Peru
e-mail: C19863@utp.edu.pe

D. A. Flores-Córdova · R. Ipanaqué-Chero · R. Velezmoro-León
Universidad Nacional de Piura, Urb. Miraflores s/n Castilla, Piura, Peru
e-mail: dflores@un.edu.pe

R. Ipanaqué-Chero
e-mail: ripanaquec@unp.edu.pe

R. Velezmoro-León
e-mail: rvelezmorol@unp.edu.pe

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_74

1 Introduction

There is the presence of Mathematics in everything we look at in our environment and in the activities we carry out in everyday life, but not all of them are evident and not all people perceive it in the same way [10]. Teachers are the ones who give life to mathematics in the learning of students; that is why it is important that they are able to identify situations in nature, in man-made constructions, whether concrete or abstract, where mathematics intervenes.

Currently, the accumulation of information and technological advances produce an acceleration in interactions and social dynamics. They have been incorporated in all areas, such as education, as learning tools. By incorporating TICs in education, it has generated a new learning environment [7], making it more attractive due to the way it interacts, generates interest in the student and because it develops digital skills.

Among the factors that have contributed to the incorporation of technology in educational institutions [3] are the accessibility provided by TIC, its pedagogical potential, easy user interaction and pressure from society to acquire digital skills.

An educational need is the teaching of spatial geometry because our environment is closely related to it. We move in a three-dimensional world, so it is important for the student to learn to represent and describe solids. Highlighting among them the polyhedra for their structural aspect, since they are visualized in architectural forms or in nature. These forms are even made through 3D graphics software. The ability to make representations of polyhedra allows students to develop creative thinking through logical thinking when describing, classifying, planning and executing procedures that allow modeling through concrete material or using graphic software for better manipulation and symbolization.

Achieving that the student manages to internationalize the characteristics of the real objects associated with them. The scarce content of spatial geometry in the regular basic education curriculum puts students who receive little training at a disadvantage. There are international studies of the TINSS tests that closely correlate the knowledge of geometry content with the development of mathematical, visual and deductive reasoning skills, as well as facilitating the representation of concepts and relationships in other branches of mathematics [11].

Currently, there is a recognition of the importance of spatial geometry in the education of students [7] given by the rise of dynamic geometry environments in 3D. These are allowing students to perform manipulations and constructions to generate new knowledge, surpassing the limitations of the manipulable materials used in classes due to their rigidity. Although, the concrete material manipulated by the students has shown to some extent effectiveness [5] such as a better visualization when making cuts [2] and very useful for calculating the volume.

Therefore, the teacher must incorporate new technological advances such as digital devices and applications available in the educational field for the teaching of polyhedra. Given what has been described, the research question arises: Can students generate new polyhedra from a cube using GeoGebra for their construction, visualization and description of their characteristics?

The objective of the research is to provide students and teachers with a dynamic way of interacting with GeoGebra to build new polyhedra from a cube. Through its manipulation, it allows them to visualize its characteristics.

2 Construction of the Polyhedra with GeoGebra

The learning of mathematics, using technological means, favors learning, that is, in the search for knowledge about the object of study, connections between its elements; they also activate and motivate students toward study [1].

In this work, GeoGebra will be used for all its benefits and its easy interaction with the student and the teacher. It is a free mathematical software for all educational levels, created by Markus Hohenwarter in 2001 at the University of Salzburg and later at the University of Atlantis. Its open source (GNU GPL) and uses the Java platform guaranteeing its portability to Windows, Linux, Solaris or Mac OS X systems. GeoGebra combines graphic and symbolic representations, dynamically gathers geometry, algebra, statistics, calculation in graphic registers, analysis and of spreadsheets organization. It was created in 2001 and is extremely user-friendly.

In this sense, GeoGebra is an excellent tool for the teaching and learning process of mathematics. In addition, it helps students to stimulate and develop creativity by discovering, recognizing, identifying, seeking new relationships and building knowledge.

Using GeoGebra, a cube will be built first in the first octant; previously, they will activate the 3D view (see Fig. 1 (left)).

We will enter point $A(0, 0, 0)$ (see Fig. 1(right)). In the 2D view, they will activate a slider in the interval [0, 20] with an increment of 0.5 and an input box associated with the slider, allowing to manipulate the edge of the cube (see Fig. 2(left)).

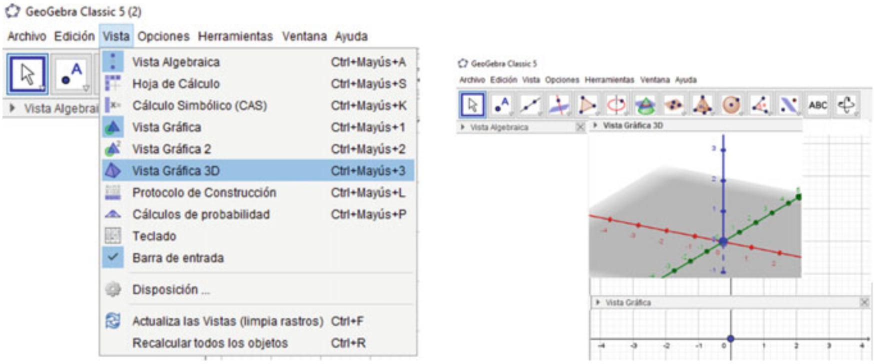
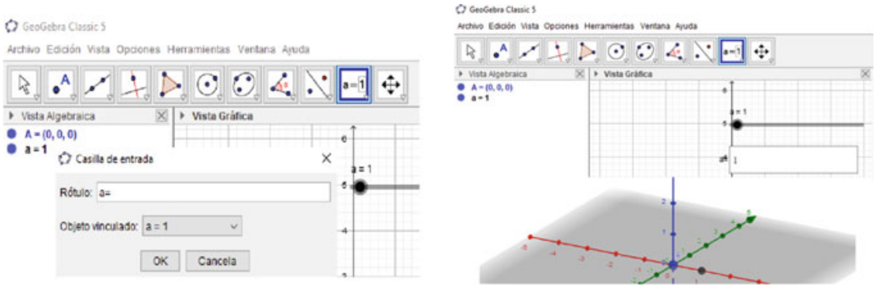

GeoGebra Classic 5 (2)
Archivo Edición Vista Opciones Herramientas Ventana Ayuda
Vista Algebraica Ctrl+Mayús+A
Hoja de Cálculo Ctrl+Mayús+S
Cálculo Simbólico (CAS) Ctrl+Mayús+K
Vista Gráfica Ctrl+Mayús+1
Vista Gráfica 2 Ctrl+Mayús+2
Vista Gráfica 3D Ctrl+Mayús+3
Protocolo de Construcción Ctrl+Mayús+L
Cálculos de probabilidad Ctrl+Mayús+P
Teclado
Barra de entrada
Disposición ...
Actualiza las Vistas (limpia rastros) Ctrl+F
Recalcular todos los objetos Ctrl+R
Vista Algebrai
GeoGebra Classic 5
Archivo Edición Vista Opciones Herramientas Ventana Ayuda
ABC
Vista Algebraica
Vista Gráfica 3D
Vista Gráfica

Fig. 1 (left) 3D graphics view. (right) Point $A(0, 0, 0)$

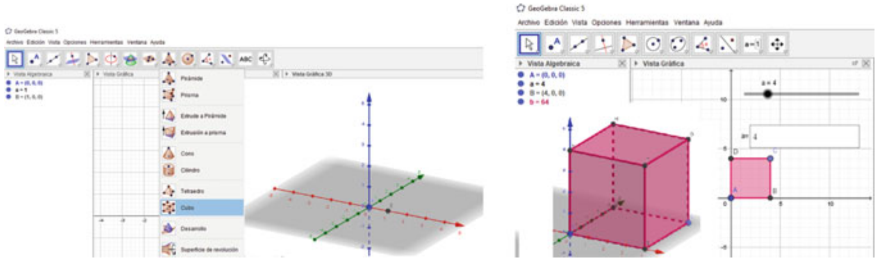


A = (0, 0, 0)
a = 1

Rótulo: a=

Objeto vinculado: a = 1

Fig. 2 (left) Slider a. (right) Point $B(a, 0, 0)$ as a function of the slider



A = (0, 0, 0)
a = 1
B = (1, 0, 0)

A = (0, 0, 0)
a = 4
B = (4, 0, 0)
b = 64

Fig. 3 (left) Cube command, which allows us to build the regular hexahedron. (right) Construction of the cube knowing the edge

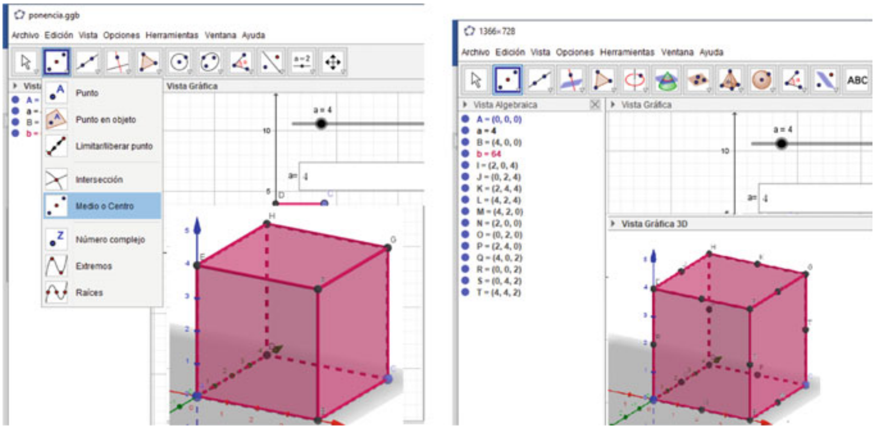
Let's enter point $B(a, 0, 0)$ the edge of the cube (see Fig. 2(right)). Taking the two points, we can build the cube the edge of the cube (see Fig. 3(left)). We select points A and B (see Fig. 3(right)).

We can see that a cube was built, and in the algebraic view, you can verify the dimension of the cube's edge and the volume. The following question is formulated: Can a new polyhedron be built from a cube if we know the midpoints of the edges? Using the midpoint command, the vertices of the new polyhedron are found (see Fig. 4(left) and (right)).

The regular hexahedron is a convex and regular polyhedron, whose characteristics:
Number of vertices: 8
Number of faces: 6
Polygon that make up the faces: squares
Number of edges: 12
Total area: $6L^2$
Volume: L^3
It is verified that it satisfies the Euler equation: $C + V - A = 2$.

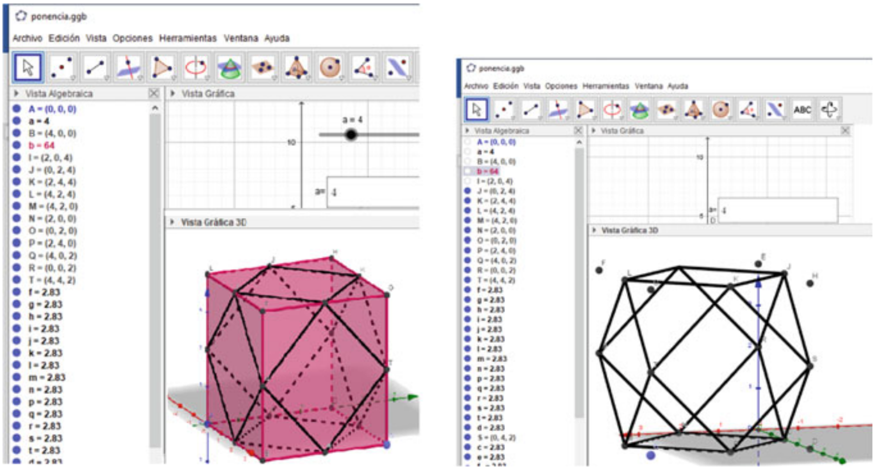
Proceeding to join the vertices by means of edges to build the new polyhedron (see Fig. 5(left)).

We proceed to hide the volume of the regular hexahedron to visualize the new polyhedron (see Fig. 5(right)).



A = (0, 0, 0)
a = 4
B = (4, 0, 0)
b = 64
I = (2, 0, 4)
J = (0, 2, 4)
K = (2, 4, 4)
L = (4, 2, 4)
M = (4, 2, 0)
N = (2, 0, 0)
O = (0, 2, 0)
P = (2, 4, 0)
Q = (4, 0, 2)
R = (0, 0, 2)
S = (0, 4, 2)
T = (4, 4, 2)

Fig. 4 (left) Using command midpoint given two points. (right) The midpoints of the edges of the regular hexahedron



A = (0, 0, 0)
a = 4
B = (4, 0, 0)
b = 64
I = (2, 0, 4)
J = (0, 2, 4)
K = (2, 4, 4)
L = (4, 2, 4)
M = (4, 2, 0)
N = (2, 0, 0)
O = (0, 2, 0)
P = (2, 4, 0)
Q = (4, 0, 2)
R = (0, 0, 2)
T = (4, 4, 2)
f = 2.83
g = 2.83
h = 2.83
i = 2.83
j = 2.83
k = 2.83
l = 2.83
m = 2.83
n = 2.83
p = 2.83
q = 2.83
r = 2.83
s = 2.83
t = 2.83

A = (0, 0, 0)
a = 4
B = (4, 0, 0)
b = 64
I = (2, 0, 4)
J = (0, 2, 4)
K = (2, 4, 4)
L = (4, 2, 4)
M = (4, 2, 0)
N = (2, 0, 0)
O = (0, 2, 0)
P = (2, 4, 0)
Q = (4, 0, 2)
R = (0, 0, 2)
T = (4, 4, 2)
f = 2.83
g = 2.83
h = 2.83
i = 2.83
j = 2.83
k = 2.83
l = 2.83
m = 2.83
n = 2.83
p = 2.83
q = 2.83
r = 2.83
s = 2.83
t = 2.83
d = 2.83
S = (0, 4, 2)
c = 2.83
e = 2.83

Fig. 5 (left) Joining the midpoints by edges. (right) New 14 faces convex polyhedron

When we start from a cube with edge L, the new polyhedron has 14 faces of which 6 of its faces are square with side $\frac{\sqrt{2}}{2}L$ and 8 equilateral triangular faces with $\frac{\sqrt{2}}{2}L$ (see Fig. 6). To calculate the volume of the new 14 faces convex polyhedron, we must calculate the volume of the pyramid shown in Fig. 7; the volume of said pyramid is $\frac{L^3}{48}$, and the volume of the new 14 faces non-regular convex polyhedron is: $\frac{5}{6}L^3$.

The characteristics of the 14-sided polyhedron are:
Number of vertices: 12
Number of faces: 14

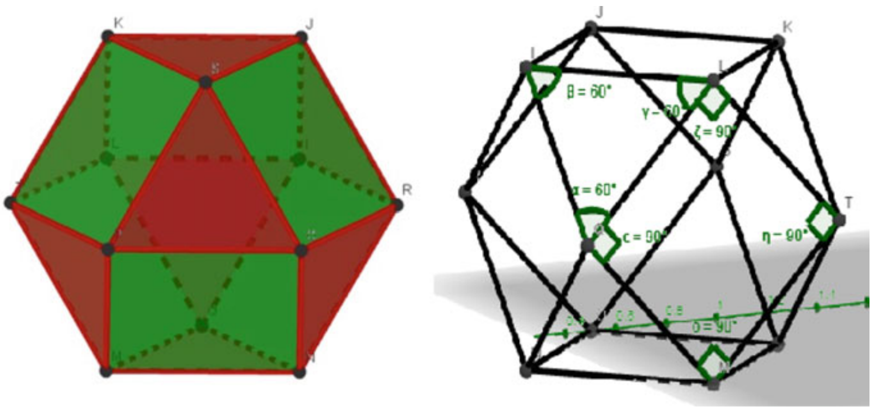


Fig. 6 (left) 14 faces irregular convex polyhedron. (right) New polyhedron with 14 faces built from the cube with side L, 6 are squares with side $\frac{\sqrt{2}}{2}L$ and 8 equilateral triangles with side $\frac{\sqrt{2}}{2}L$

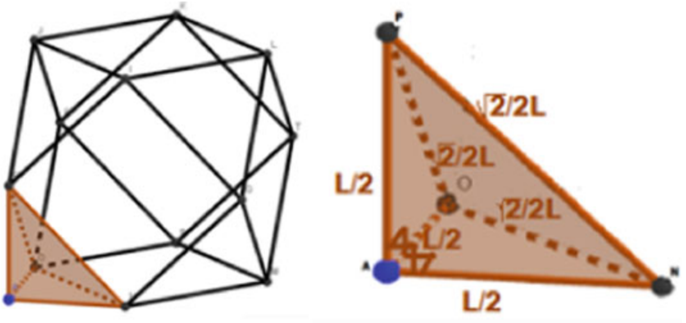


Fig. 7 Pyramid to which we will calculate its volume

Number of edges: 24
Total area: $\left(3+\sqrt{3}\right)L^2$ We verify that it satisfies Euler's equation: $C + V - A = 2$.

Building a new polyhedron from the previous polyhedron finding the midpoints of the edges, we obtain the irregular convex polyhedron with 26 faces (see Fig. 8(left)). The characteristics of this new convex polyhedron are:

Number of vertices: 24
Number of faces: 26
Number of edges: 48
Total area: $\left(\frac{6+6\sqrt{2}+\sqrt{3}}{4}\right)L^2$
We verify that it satisfies the Euler equation: $C + V - A = 2$.

Using the cube of edge L, the new polyhedron has 26 faces, of which 6 of its faces are squares with side $\frac{L}{2}$, 12 are rectangles of dimensions $\frac{L}{2}$ and $\frac{\sqrt{2}}{4}L$; finally, 8 equilateral triangular faces of side $\frac{\sqrt{2}}{4}L$ (see Fig. 8(center)). To calculate the volume

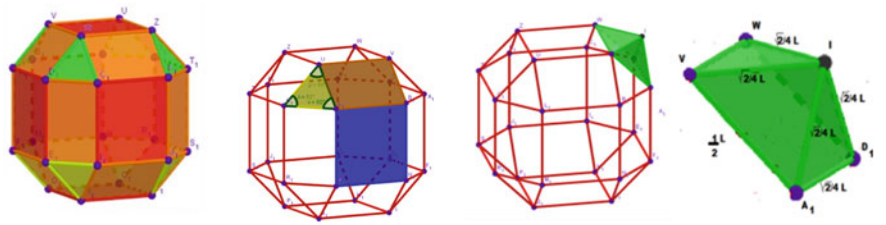


Fig. 8 (left) 26 faces irregular convex polyhedron. (center) Identification of the different types of faces that exist in the 26-face convex polyhedron, calculate the total area. (right) On the right, we can see the pyramid whose volume we will calculate

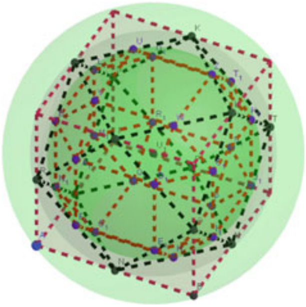


Fig. 9 Regular hexahedron, irregular convex polyhedron with 14 and 26 faces, inscribed in spheres with radii L, $\frac{\sqrt{2}}{2}L^2$ and $\frac{\sqrt{6}}{4}L$, respectively

of the new 26 faces convex polyhedron, we have to calculate the volume of the pyramid shown in Fig. 8(right), whose value is: $\frac{1}{96}L^3$. The volume of the new 26 faces non-regular convex polyhedron is: $\frac{79}{96}L^3$.

Analyzing each of the polyhedra, it is found that they are inscribable (see Fig. 9); doing the respective analysis, it is obtained that: The cube of edge L is inscribed in a sphere of radius $\frac{\sqrt{3}}{2}L$. The 14 faces irregular convex polyhedron is inscribed on a sphere of radius $\frac{\sqrt{2}}{2}L$. The 26 faces irregular convex polyhedron is inscribed on a sphere of radius $\frac{\sqrt{6}}{4}L$.

3 Conclusions

Starting from a cube with edge L, an irregular convex polyhedron with 14 faces can be constructed taking the midpoints of the cube as vertices. An irregular convex polyhedron with 14 faces is generated that has the peculiarity of having 6 faces that are square on each side $\frac{\sqrt{2}}{2}L$ and 8 faces that are equilateral triangles with side $\frac{\sqrt{2}}{2}L$. Also, their area is 14 faces is $\left(3+\sqrt{3}\right)L^2$, and their volume is $\frac{5}{6}L^3$.

Considering the 14 faces irregular convex polyhedron and finding the midpoints of each of its edges, we can build an irregular convex polyhedron with 26 faces of which 6 of its faces are squares of side $\frac{1}{2}L$, 12 are rectangles of dimensions $\frac{1}{2}L$ and $\frac{\sqrt{2}}{4}L$, finally, 8 equilateral triangular faces of side $\frac{\sqrt{2}}{4}L$. Their total area and volume are $\left(\frac{6+6\sqrt{2}+\sqrt{3}}{4}\right)L^2$ and $\frac{\sqrt{6}}{4}L$, respectively.

The ratio between the volumes of the 14 faces irregular convex polyhedron and the cube is $\frac{5}{6}$, and between the 26 and 14 faces irregular convex polyhedron is $\frac{79}{80}$. While, the ratio between their radii of the spheres that inscribe the 14 faces irregular convex polyhedron and the cube is $\frac{\sqrt{6}}{3}$ and between the radii of the spheres that inscribe the 26 and 14 faces irregular convex polyhedron is $\frac{\sqrt{3}}{2}$.

In 14 and 26 faces irregular convex polyhedra constructed from a cube, students can find their characteristics using their knowledge of plane geometry, allowing you to give a better argument for your results by making generalizations from a cube with arbitrary side l [4].

Some research works indicate that the use of dynamic geometry programs may not be positive for students [5]. For the situation to be feasible, the activities that are programmed must promote the learning process of the students through the understanding of the structures and characteristics of the polyhedra that they themselves generate. The spatial geometry teaching environment using GeoGebra software requires the teacher to analyze whether students understand the geometric properties of polygons and geometric solids. Also, students must be verified by the properties using the [8] software, taking advantage of the different perspectives that GeoGebra offers when manipulating the object. By allowing them to construct the new polyhedra and determine their respective characteristics, there would be a positive correlation between the use of dynamic geometry software and greater visualization capabilities [9].

References

1. Álvarez M, Almeida B, Villegas E (2014) El proceso de enseanzañaprendizaje de la matemática. Pueblo y Educación, La Habana
2. Accascina G, Rogora E (2006) Using Cabri3D diagrams for teaching geometry. Int J Technol Math Educ 13(1):11–22. https://www.semanticscholar.org/paper/Using-Cabri3D-Diagrams-For-Teaching-Geometry-Accascina-Rogora/06372bfaebb4d98156d8fe5fab8d09e25afa7129
3. Bates A (2004) La transformación de las universidades a través de las TIC: discursos y prácticas. Editorial UOC, Barcelona https://www.uoc.edu/dt/esp/sangra1104.pdf
4. Cardozo F (2019) El uso de geogebra para el estudio de poliedros, como estrategia para potenciar los niveles de argumentación. Universidad Autónoma de Manizales, Colombia. http://repositorio.autonoma.edu.co/jspui/handle/11182/1033?locale=en
5. Clements D, Battista M (1992) Geometry and spatial reasoning. Handbook Res Math Teach Learn 1:420–464. https://psycnet.apa.org/record/1992-97586-018
6. Custodio J, Suárez N (2014) Evolución de las tecnologías de la información y comunicación en el proceso de enseñanza y aprendizaje. Revista Vínculos 11(1):209–220. https://doi.org/10.14483/2322939X.8028
7. David M, Tomaz V (2012) The role of visual representations for structuring classroom mathematical activity. Educ Stud Math 80(3):413–431. https://www.jstor.org/stable/41485989

8. De Oliveira W, Meneguelo N (2015) Uso do geogebra 3d para o ensino de poliedros. V jornada de educação matemática. UERJ-Faculdad De formação de professores. http://feap.edu.br/wp-content/uploads/2017/02/Artigo_Wendel_Uerj.pdf
9. Güven B, Kosa T (2008) The effect of dynamic geometry software on student mathematics teachers'spatial visualization skills. Turkish Online J Educ Technol 7(4):100–107. https://files.eric.ed.gov/fulltext/EJ1102930.pdf
10. Palmer M (2018) Las matemáticas de la vida cotidiana. La realidad como recurso de aprendizaje y las matemáticas como medio de comprensión. Miradas Matemáticas, Madrid España
11. Tatsuoka K, Corter J, Tatsuoka C (2004) Patterns of diagnosed mathematical content and process skills in TIMSS-R across a sample of 20 countries. Am Educ Res J 41(4):901–926

Harmonize: A Comprehensive Patient and Provider Connectivity Solution for the Management of Mental Disorders

Dion Wayne Pieterse and Sampson Akwafuo

Abstract Mental illness and associated disorders are deep social problems that are largely ignored. Individuals with mental illnesses face many obstacles such as stigma, prejudice, and unemployment, which dissuades them from seeking help. The emergence of COVID-19 brought light to the importance of mental health. Current online patient–provider networking services act as the proverbial phone book, and finding the right provider can be a shot in the dark. There is a lack of opportunity to converse, connect or interact with providers without paying for a formal appointment. As a result, patients have a hard time finding a compatible provider. In this paper, we present details of a comprehensive journal-like patient and provider connectivity solution for the management of mental disorders. In addition to providing a platform for individuals with mental disorders to confidentially connect with medical service and insurance providers, it allows for group forums among peers. Communication and trust can be enriched with a networking application that allows patients (under an anonymous alias) and providers to freely monitor, like mention and interact with one another before initial contact. Building a privacy-focused networking platform on top of well-known communication mediums like forums and blogs can enhance communication, visibility, and understanding. Better communication, trust, and understanding lead to high-quality therapy.

Keywords Mental health · Digital journal · Health management system · Patient and provider networking tool

1 Introduction

Mental illness is a social problem that is largely ignored. The general cost of mental illness on an individual and economic level is constantly growing. The most common mental health conditions are various types of anxiety and depression. Other preexisting health conditions and co-infections may also lead to mental illness overtime [1].

D. W. Pieterse (✉) · S. Akwafuo
California State University, Fullerton, CA 92831, USA
e-mail: dionpieterse@csu.fullerton.edu

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_75

Popular treatments for mental health ailments include cognitive behavioral therapy (CBT) and writing therapy (journaling). Research by Xu et al. [2] reported that as of 2007, there were 450 million of us living with some form of mental illness. The study states that by 2020, mental disorders will account for roughly 15% of the total global cost of diseases. The National Alliance on Mental Illness (NAMI) reports [3] that 1 in 5 Americans experience mental illness annually as of March 2021. Mental illness can take a toll on society and incur devastating costs in numerous ways. Some of these costs are more visible and impactful on the everyday person, and others are less obvious than those who suffer from it. A conservative estimate for the economic cost of severe mental illness alone is $317 billion, which does not include patients with more than one underlying condition, the homeless, the imprisoned, or those that have died early because of it. A large percentage of mental health cases are anxiety, depression, and post-traumatic stress disorder. According to the National Alliance of Mental Illness (NAMI) [3], anxiety disorders, major depressive episodes, post-traumatic stress disorder, obsessive–compulsive disorder account for 19.1%, 7.8%, 3.6%, and 1.2%, respectively, for all cases in America. These conditions account for 31.7% of all mental health cases in America as of March 2021. Cognitive behavioral therapy (CBT) is a mental health treatment that therapists employ. CBT is a typical verbal therapy used by itself, or in combination with other therapies, used in a one-on-one setting with patient and therapist. The patient purposely exposes themselves to situations that trigger discomfort. Patient and therapist analyze these uncomfortable situations to teach patient awareness and cope with negative thoughts and emotions. Cognitive behavioral therapy has risen to become a first choice for treating anxiety. According to a study by Nielsen et al. [4], CBT is a viral therapy employed globally. It has been shown to be effective in treating anxiety and associated disorders. It is also cost-effective.

2 Literature Review

2.1 Provider Awareness Beyond In-Network Scope

Finding affordable health insurance is a growing challenge in the USA today. The Affordable Care Act (ACA) was enacted to combat rising healthcare costs and expand cheap health insurance. According to a study by Rowan [5], the increased cost proved to be a significant barrier to many who had private insurance and mental illness. The price was a significant barrier for those with serious mental illness who sought treatment for all types of insurance. Two-thirds of out-of-pocket patient expenditure went toward prescription drugs. Simply increasing eligibility and availability of insurance plans will not reduce these out-of-pocket expenditures. The viability of ACA lies in the legal fine print, and there is much work to be done. The ACA has made strides to increase mental health coverage for the uninsured and make their sponsored plans more financially attractive for employers to adopt. There is still a need to address laws that regulate how insured patients end up paying hefty out-of-pocket fees. These high out-of-pocket costs have historically been a deterrent for the mentally ill and have resulted in greater dependence on public health insurance, especially for the poor. Rowan [5] concludes that simply increasing the availability of health insurance coverage does little to make health insurance more affordable. The lack of affordability is solved by closing legal loopholes that enable insurers and providers to dump high out-of-pocket costs on patients. According to a recent study, Sun et al. [6] point out that it is reasonable for a patient to assume all providers and services in the hospital their insurance company recommended are in-network, but that is not true. Many providers working in a patient's in-network facilities are out-of-network, and notification systems in place to make patients aware of providers' network status are questionable. This lack of transparency leads to surprise billing for patients.

2.2 Advantages of a Digital Journal for Mental Health Therapy

Despite how technological society has become, there is a surprising lack of digital journals mental health systems online. Many therapists still tell their patients to write their thoughts or daily activities in a notebook. Once journaling becomes a digital feature, it can quickly and efficiently be integrated into a more extensive system incorporating other therapeutic methodologies. CBT can be coupled with journaling to form a type of therapy called cognitive behavioral writing therapy (CBWT). This hybrid therapy has proven invaluable for many who suffer from anxiety and depression. According to research done by Van der Oord et al. [7], the use of computer-aided CBWT for children who had post-traumatic stress disorder (PTSD) and depression was very effective and long-lasting. Even after six months since the initial treatment, the children produced positive feedback from the treatment. Interestingly, Van der Oord et al. [7] describe a contention in the study by those who believed handwritten CBWT might be more effective than computer-aided CBWT. The analysis performed in the survey debunked this hypothesis. There was no evidence to show how the patient's responses were conveyed (written, typed, or verbal), which made any difference in the effectiveness of CBWT.

2.3 Using Natural Language Processing (NLP) for Mental Health Therapy

The amount of data that pertains to individual patients can quickly grow into massive data sets or countless pages of information that the therapist will constantly have to maintain and analyze. Scouring over documents and data can be tiring for any therapist. Worse, they could miss vital signs and information that could aid them in developing a meaningful treatment for their patients. According to Le et al. [8], computer analysis via NLP of patient records proves a practical patient risk assessor. Le explains that NLP saved time and money to effectively assess patient risk factors from large volumes of text. Usually, the same volume of text would require analysis by experts over more extended periods and cost a lot more money. Interestingly, research by Le et al. [8] is reinforced by a study conducted by Cook et al. [9]. Cook et al. [9] found NLP's analysis of patient data to be an effective predictor of patient suicide. Cook et al. [9] also echo Le's research by stating that NLP is accurate and saves money when analyzing massive patient data. Cook et al. [9] highlight the value of utilizing NLP on data sent from the patient to the provider over secure channels. NLP could be used to detect suicidal tendencies in the patient's language.

3 Methodology

Harmonize is a web application that enhances communication, understanding, and trust between patients and providers. The application increases providers' visibility and promotes interaction with patients through two methods of online interaction, a **blog** and a **forum**. Patients have a privacy-focused journal (blog), while a blog is provided to the providers to market their services. The forum will create an environment where patients and providers can interact and evaluate each other in group conversations. The application employs social networking features to enhance effective and direct communication and visibility, including liking user entries and mentioning users. The use of NLP further enhances the ability of the therapist to analyze large volumes of their patient's monitored data. All patients will be identified anonymously for privacy. Providers are not anonymous and are identified by their professional name. The user will be presented with the home page, a general landing page for site visitors. The user will have the option to register a new account or log in as an existing user. The registration form will allow users to make their account a "patient" or "provider" user type. Upon registering as a new user, they are automatically logged into their account and redirected to the home page. Upon creating a new account, the new user will have to navigate to the "Edit Account" page, which allows them to enter critical information that will enhance connectivity with other registered patients and providers. If they are actively seeking a provider, the user can enter their general information, choose to make their account non-searchable, choose their current mental health conditions, choose their insurance company, and write a bio about themselves. Every user has a "Landing Page." The landing page is the primary user page for others to visit when looking for another user. It acts as the launching point for everything concerning that user. Page options include:

- View user's blog.
- Choose to monitor a user.
- Grant Privacy Access to a user.
- View if a user is actively seeking a provider or accepting new patients.

- View if the blog is searchable (indicating access status to the entire blog).

The patient or provider has access to their journal and blog, respectively. The users' journals and blogs are the same and have different user types (to signify different usage). Each user can write an entry, which can include an image or not. Each blog entry can be "liked" or "unliked" by other users. The user has complete control to set the privacy control of each blog entry to "public" or "private." The user can edit or remove any blog entry they create. When providers are granted private access to a patient's journal, they will see both private and public entries. The provider will also have a color-coded sentiment analysis bar visible on each journal entry for quick visual sentiment interpretation. The provider can click on a "View Analysis" button for each journal entry, which takes them to a new page that details the sentiment analysis and name entity recognition for each journal post. This feature enhances the provider's ability to interpret quickly and single out concerning journal entries of potential clients (since they were granted privacy access). Every registered user has access to the public forum. The public forum consists of "Rooms," which hold conversations about a specific subject. The author of a room can edit or remove any remove they have made. Upon visiting a room, a user can click on a "Conversation," which contains a dialogue between patient and provider user types in response to a conversation starter question. A starter question is always entered by the author of the conversation upon creation. The splashboard is an interface that allows users to quickly access valuable data and connections facilitated by the application's social networking features and data relationships. The splashboard has two sections, "General Data Services and Provider Data Services." Options for the "General Data Services" with different functionalities.

Every registered user has a search feature in the navigation, which they can use to search the public forums. The search results will render a paginated list of responses with a breadcrumb link chain of the room, conversation, and response.

Activities

1. Create wireframe and OO class diagrams for application.
2. Setup the PostgreSQL server and create the project database.
3. Create the project package, and install all dependencies.
4. Build the back-end logic first, on top of a basic front-end skeleton.
5. Once the back-end is complete and functioning, complete the front-end design.
6. Perform testing on the application.
7. Write the final report documentation for the project.
8. Present and demonstrate the project.

The applications were developed using Python. The back-end runs on Flask web framework. The front-end uses HTML5, Bootstrap 4 CSS Framework. The database management system is PostgreSQL. The graphic and designs were done using Adobe Photoshop and Illustrator. A minimum RAM requirement of 2 GB is suggested to efficiently run it.

4 Case Study and Example Usage

Upon visiting the home page of the application, a new user has the option to register an account by clicking register, or if they already have an account, they can login. This is shown in Fig. 1.

Once logged into the application, the user can update their account information and enter details about their condition(s) and insurance information. See Fig. 2.

Users have access to their blog, the forum, and their customized splashboard under the navigation option "Account/Services" They are also able to view the main public room and make contributions through this screen. This is shown in Fig. 3.

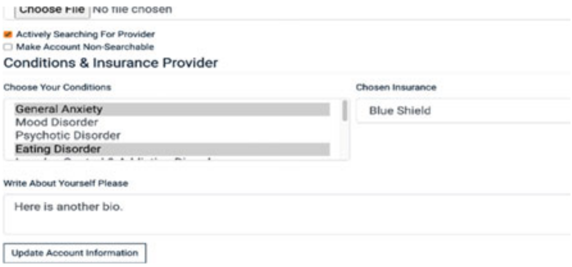
Every user has their own landing page, which acts as an information hub for that user, and a staging point to access that user's blog. Every user landing page has a button menu which allows visiting users the ability the grant that user privacy access to view their private blog entries. There is a button to monitor that user, as well as alerts that indicate if the user's blog is visible to others, and if that user is seeking therapy (if a patient user type) or accepting patients (if a provider user type) (Fig. 4).

Each user's blog entry can be public or private, and only users who the blog owner has granted privacy access to, can view their private entries or sentiment analysis (if a provider user type). Every blog entry can be liked or unliked, and users can be mentioned by their user alias. Each blog entry can be edited or removed by the author. If the user who was granted Provider Privacy Access, then they can view the patient's sentiment analysis data per journal entry. For quick visual interpretation of sentiment, there is a color bar visible for every journal entry. These activities are shown in Figs. 5 and 6.

Upon clicking on View Analysis, the user will have access to a more detailed sentiment analysis breakdown and Named-Entity Recognition (NER) per sentence. NER is customized to recognize numerous types of entities and visually highlight them for the reader.

Fig. 1 Navigation links

Fig. 2 Editing an account



No file chosen

☑ Actively Searching For Provider
□ Make Account Non-Searchable

Conditions & Insurance Provider

Choose Your Conditions

General Anxiety
Mood Disorder
Psychotic Disorder
Eating Disorder

Chosen Insurance

Blue Shield

Write About Yourself Please

Here is another bio.

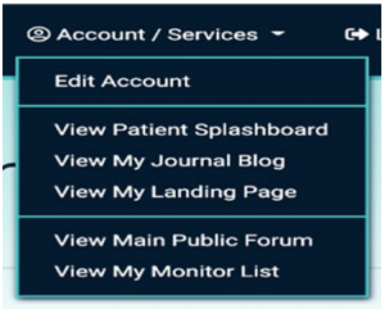
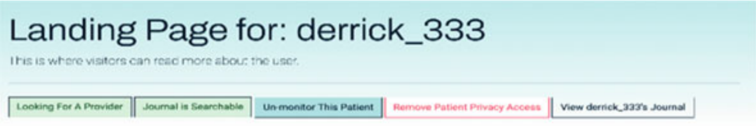


Fig. 3 Account/services (Navigation)


Landing Page for: derrick_333

This is where visitors can read more about the user.

Fig. 4 Landing page

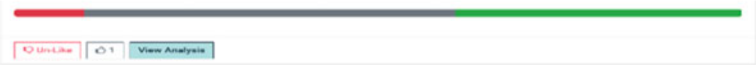
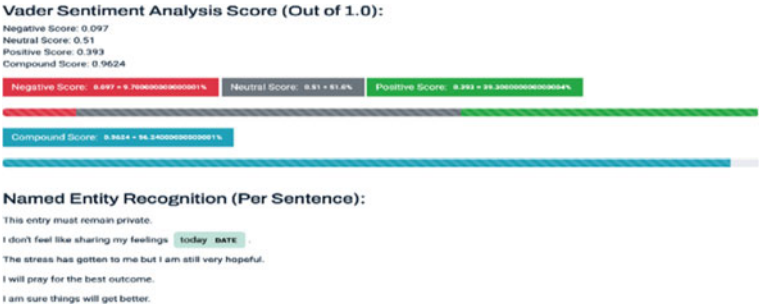


Fig. 5 Sentiment analysis


Vader Sentiment Analysis Score (Out of 1.0):

Negative Score: 0.097
Neutral Score: 0.51
Positive Score: 0.393
Compound Score: 0.9624

Negative Score: 0.097 = 9.700000000000001%
Neutral Score: 0.51 = 51.0%
Positive Score: 0.393 = 39.300000000000004%

Compound Score: 0.9624 = 96.24000000000001%

Named Entity Recognition (Per Sentence):

This entry must remain private.

I don't feel like sharing my feelings today DATE .

The stress has gotten to me but I am still very hopeful.

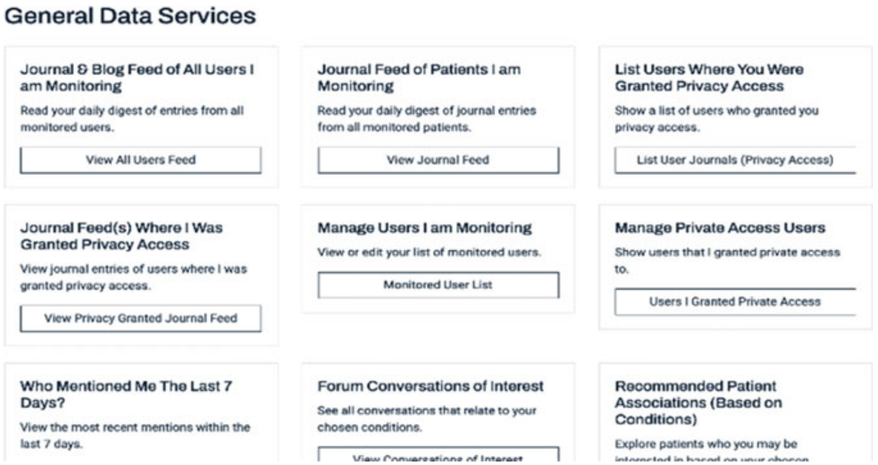
I will pray for the best outcome.

I am sure things will get better.

Fig. 6 Sentiment analysis details

Every user has access to the application forum where patient and provider user types can freely converse and interact. The forum contains Rooms, which hold related conversation. Every conversation contains a chain of responses related to that conversation. Each response can be liked or unliked, and users can be mentioned by their user alias. Every response created by a use can be edited or removed by that same user. Every user has access to their own splashboard by clicking the "View Patient Splashboard" or "View Provider Splashboard" (depending on their user type). The splashboard is a comprehensive data delivery interface that allows the user quick access to specific data regarding their social networking connections. The data is generated based on what information the user has entered for their account, the users they are monitoring, the users they have granted privacy access to, and which blog entries or forum responses they have liked. See Fig. 7.

Some data services include: (1) Journal and Blog Feed of All Users under monitor (2) Journal Feed of Patients I Am Monitoring (3) List of Users with Privacy Access (4) Manage Users I am Monitoring (5) Manage Private Access Users (6) Who Mentioned the current user Within The Last Week (7) Forum Conversations of Interest (8) Recommended Other Patient Associations (Based on Conditions) (9) Forum Response Feed of All Users I Am Monitoring (10) Forum Response Feed of Patients I am Monitoring, and other functions described in the user documentation. The admin has access to the data management system, which is a user interface that allows full editing capability to the database tables, as well as various customizable features for searching, exporting data sets as certain file formats, sorting data, and filtering data (Fig. 8).



General Data Services

Journal & Blog Feed of All Users I am Monitoring
Read your daily digest of entries from all monitored users.
View All Users Feed

Journal Feed of Patients I am Monitoring
Read your daily digest of journal entries from all monitored patients.
View Journal Feed

List Users Where You Were Granted Privacy Access
Show a list of users who granted you privacy access.
List User Journals (Privacy Access)

Journal Feed(s) Where I Was Granted Privacy Access
View journal entries of users where I was granted privacy access.
View Privacy Granted Journal Feed

Manage Users I am Monitoring
View or edit your list of monitored users.
Monitored User List

Manage Private Access Users
Show users that I granted private access to.
Users I Granted Private Access

Who Mentioned Me The Last 7 Days?
View the most recent mentions within the last 7 days.

Forum Conversations of Interest
See all conversations that relate to your chosen conditions.
View Conversations of Interest

Recommended Patient Associations (Based on Conditions)
Explore patients who you may be interested in based on your chosen

Fig. 7 Splashboard

Fig. 8 Administrator

5 Conclusion

The services for patients to discover, interact with, and learn about providers are lacking and underdeveloped on many levels. Finding responsive and trusted insurance companies is a challenge to patients. Many patients with health insurance have access to in-network providers and have limited visibility and affordable access to an out-of-network provider. There is a high chance that in-network mental health patients will have out-of-network services, so they must have visibility of all providers in their geographic location regardless of network. Many of the online provider networking services do not promote communication and interaction with patients without payment. Current applications provide services that cater specifically to providers and help them market their business. These marketing tools are delivered on static profile pages and do not involve social interaction with potential patients. Many of the tools are primitive and limited. There is no dynamic communication platform between patient and provider. Communication and trust are two of the most critical factors for a patient to receive quality therapy from a provider. Providers have access to sentiment analysis tools that enhance and aid their diagnosis and treatment strategies of potential and current patients. The application provides services free of charge to promote interaction with its users and increase the likelihood of patients finding the best match provider to help them with their mental health condition(s). A system that enhances the efficiency of patients' and providers' connectivity increases the likelihood of effective treatment and healing. Patients who find effective therapy become productive citizens, enrich the economy, and enhance their lives and society as a whole.

References

1. Akwafuo S, Abah T, Oppong J (2020) Evaluation of the Burden and intervention strategies of TB-HIV co-infection in West Africa. J Infect Dis Epidemiol 6(4). https://doi.org/10.23937/2474-3658/1510143
2. Xu J, Wang J, Wimo A, Qiu C (2016) The economic burden of mental disorders in China, 2005–2013: implications for health policy. BMC Psychiatry 16(1). https://doi.org/10.1186/s12888-016-0839-0
3. NAMI (2021) Mental health by the numbers, https://www.nami.org/mhstats
4. Kerstine S, Nielsen K, Vangkilde S, Wolitzky-Taylor KB, Daniel SIF, Hageman I (2016) An investigation of general predictors for cognitive-behavioural therapy outcome for anxiety disorders in a routine clinical setting. BMJ Open 6:10898. https://doi.org/10.1136/bmjopen-2015
5. Kathleen Rowan LAB, McAlpine DD, Access and cost barriers to mental health care, by insurance status, 1999–2010
6. Sun EC, Mello MM, Moshfegh J, Baker LC (2019) Assessment of out-of-network billing for privately insured patients receiving care in in-network hospitals. JAMA Intern Med 179(11):1543–1550. https://doi.org/10.1001/jamainternmed.2019.3451
7. Van Der Oord S, Lucassen S, Van Emmerik AAP, Emmelkamp PMG (2010) Treatment of post-traumatic stress disorder in children using cognitive behavioural writing therapy. Clin Psychol Psychother 17(3):240–249. https://doi.org/10.1002/cpp.670

8. Van Le D, Montgomery J, Kirkby KC, Scanlan J (2018) Risk prediction using natural language processing of electronic mental health records in an inpatient forensic psychiatry setting. J Biomed Inform 86:49–58. https://doi.org/10.1016/j.jbi.2018.08.007
9. Cook BL, Progovac AM, Chen P, Mullin B, Hou S,Baca-Garcia E (2016) Novel use of natural language processing (NLP) to predict suicidal ideation and psychiatric symptoms in a text-based mental health intervention in Madrid. Comput Math Methods Med 2016. https://doi.org/10.1155/2016/8708434

A Post-quantum Zero-Knowledge Proof System Using Quantum Information Theory

Sonok Mahapatra, Tyler Wooldridge, and Xiaodi Wang

Abstract In recent decades, the importance of protecting computer systems and networks from information disclosure (relevant to information technology and cybersecurity fields) has risen to the utmost importance. With wide applications in subjects such as voting registration, insurance, credit card information, personal identity security, and as of recently crypto-based blockchains, the field is becoming increasingly significant. Due to the perpetual and expanding reliance on computer systems, the way that we handle and send our data is vital. Improper methods of establishing privacy for secure data transmission can compromise substantial amounts of user data, making the development of high-level privacy-preserving mechanisms impervious to tampering of immense importance. For example, the existence of most cryptographic systems is threatened by the development of quantum computing, and therefore, the development of making post-quantum/quantum-resistant cryptographic systems is in great demand. In this research, unlike most current existing systems, we propose a classical to quantum mapping channel for zero-knowledge that will not be negatively affected by the existence of quantum technologies.

Keywords Wavelet transform · Quantum signaling · Grover's algorithm · Cryptography · Trees · Asymmetric key cryptography · Quantum algorithm · Reverse encryption · Quantum cryptography · Transaction verification · Proof of work · Post-quantum cryptography · Quantum channeling

S. Mahapatra (✉)
Westhill High School, Stamford, CT 06902, USA
e-mail: sonokmahapatra@gmail.com

T. Wooldridge · X. Wang
Western Connecticut State University, Danbury, CT 06810, USA
e-mail: wooldridge002@wcsu.edu

X. Wang
e-mail: wangx@wcsu.edu

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_76

1 Introduction

Hash functions which are widely employed by cryptographic security applications are used to pass information anonymously between users. These hash functions act as privacy-preserving mechanisms that ensure data being anonymous, storable, and retrievable [1]. However, a hash algorithm's effectiveness is mitigated by quantum algorithms, such as Grovers algorithm, often because hash functions produce a fixed-size output given any random-sized input [2, 3]. Grover's algorithm is a quantum computing algorithm for an unstructured search that finds with high probability the unique input, given the particular output and black-box function. Grover's algorithm uses just $O(\sqrt{N})$ open parentheses square root of N close parentheses evaluations, whereas a classical computer requires $O(N)$ calculations, where N is the size of the functions domain [3]. Even if Grover's method does not give an exponential speedup over conventional computers, when compared to other quantum computing techniques, it might be utilized to speed up a wide variety of algorithms. In particular, NP-hard completes problems that contain extensive search [1]. The augmented speed of Grover's algorithm can be used to expedite collision attacks, and therefore compromise the security of most existing zero-knowledge proof systems [4]. Applications of Grover's algorithm include provable speedups for black-box problems in a quantum query, including the collision problem. Consequently, because of the function inversion ability, the threat of collision and preimage attacks pose a great threat to cryptographic systems such as asymmetric cryptography and blockchain.

In this research, we developed a new quantum computing-resistant cryptographic security scheme to defend against the threat of collision and preimage attacks. We created a classical to quantum mappings for zero-knowledge proof of data. This security scheme was done in accordance with finding a solution to Grover's algorithm's effect on hashing. We are confident that the post-quantum nature of the qubit representations of classical data in our algorithm will defeat quantum attacks. We were also able to explore methods of data encryption and network storage using quantum mechanical properties [5, 6]. Finally, we used a pseudo-quantum representation to illustrate a peer-to-peer network that is able to send, receive, encode, and decode pseudo-quantum signals of classical data [7].

2 Preliminaries

In quantum information theory, we have a quantum channel that acts as a communication mechanism that can transmit quantum information and be manipulated using quantum information processing techniques. Due to the following quantum properties such as No-Teleportation theorem, No-Cloning theorem, No-Deleting theorem, No-Broadcast theorem, and No-Hiding theorem, quantum information theory has broad applications in quantum communications [2, 8].

In order to create a quantum channel, we must first transform our classical data into a quantum computing input format. We then create a classical to quantum mapping that outputs a quantum state of entangled qubits which can be expressed as

$$|b_0, b_1, b_2, \cdots, b_n\rangle = |b_0 \otimes |b_1 \otimes \cdots \otimes |b_n\rangle. \tag{1}$$

We can further improve on our quantum channel by packing N classical bits into a quantum state of size qubits, which is enabled by the compression of the classical bit count and therefore enable our quantum algorithm for exponential speedup over classical algorithms [8]. The figure below shows a recursive computation on an 8 classical bit system.

Algebraically, we can represent the loading of four classical bits into a state of 3 entangled quantum bits by

$$\begin{aligned}|A\rangle = |\phi_{\alpha\beta\gamma}\rangle = |\alpha\beta\gamma\rangle &= |00\rangle \otimes |b_{00}\rangle + |01\rangle \otimes |b_{01}\rangle + |10\rangle \otimes |b_{10}\rangle + |11\rangle \otimes |b_{11}\rangle \\ &\equiv |00b_{00}\rangle + |01b_{01}\rangle + |10b_{10}\rangle + |11b_{11}\rangle,\end{aligned} \tag{2}$$

where A is a matrix containing 4 classical bit values of $\{b_{00}, b_{10}, b_{01}, b_{11}\}$.

We must also optimize the data transfer from the classical domain into the quantum domain. To do so, we recall two results [6, 9]: Shannon's Capacity Theorem and the Coding Theorem. The first provides an upper bound on the rate at which information can be transmitted, and the second states that as long as the information rate is less than or equal to the channel capacity, then there is a coding technique such that information can be transmitted over the channel with an arbitrarily small probability of error. If the information rate exceeds the channel capacity, then error-free transmission is impossible. Thus, these two results dictate that we must compress the incoming bitstream in the classical domain, pass it through the channel, and then decompress the data stream at the output in the quantum domain [10].

3 Quantum Channels

3.1 Compression of Classical Data

We employ the following approach to compress the classical data before sending it through the quantum channel. Suppose we have a block of classical data of length N bits. We then compress the N bits by a factor of L, where $L = -E_S[\log(\pi)]$ is the average entropy of a bit in the incoming bit stream. If the length $N >> 1$, then a single bit is mapped to L, for $0 < L < 1$. Thus, the block of length N is mapped to $M = LN$ bits such that $0 < M < N$. The compression and decompression methods improve the data transfer by virtue of the number of stages required in the circuit. This, in turn, reduces the number of loading circuits that are needed [6, 11]. When implemented into a quantum algorithm, this circuit exhibits an exponential speedup compared to its classical counterpart. Furthermore, we must show that the circuit's time complexity is $O(\log(N))$.

3.2 Properties of Quantum Channels

We now acknowledge some of the properties of quantum channels. For our purposes, we assume that all state-spaces are finite-dimensional [11]. There are three ways we must look at this: the first is from the Schrodinger perspective, which makes use of density matrices acting on the relevant state-spaces; the second is from the Heisenberg perspective, which extends density matrices acting on H_A to the full space of operators, and the third from the classical point of view to account for the cases in which the input data are classical in nature.

In the case of Schrodinger, let H_A and H_B be Hilbert spaces of dimensions n and m, respectively. Also, let $L(H_A)$ and $L(H_B)$ denote the collections of operators acting on H_A and H_B. We then define a purely quantum channel to be a mapping $\phi : \rho(H_A) \to \rho(H_B)$ between density matrices acting on H_A and H_B such that ϕ is a positive linear map. Thus, the induced map $I_n \otimes \phi$, is a completely positive map. Furthermore, for all density matrices ρ, $\mathrm{tr}\,(\rho) = 1$. Hence, ϕ must preserve traces [8].

Since density matrices are only one type of operator, when viewing quantum channels within the context of the Heisenberg picture, they form a (proper) subset of $L(H_A)$. Therefore, in this perspective, we extend density matrices to the entire space of operators. We can do this once we have established a mapping between density matrices, making use of the linearity property and assume finite dimensions. Thus, let us consider $L(H_A)$, $L(H_B)$ and the mapping $\phi : \rho(H_A) \to \rho(H_B)$. Note that the spaces of operators are Hilbert spaces equipped with the Hilbert-Schmidt inner product. Thus, we may obtain adjoint map ϕ^* determined by the rule $\langle A, \phi(\rho)\rangle = \langle \phi^*(A), \rho\rangle$. This map takes observables on H_B to observables on H_A. Additionally, we can check that the adjoint map ϕ^* is unital; that is, $\phi^*(I) = I$, provided that it is trace-preserving.

So far, we have only considered cases for which the input data is quantum. However, we must also consider the case where the input data is classical. Therefore, we must generalize this treatment further in order to account for this. Thus, let $\phi : L(H_B) \to L(H_A)$ be a linear map between the spaces of operators such that ϕ is unital and is a completely positive map. Viewing the spaces of operators as C^*-algebras, we can then redefine our linear map to be a unital, completely positive map between C^*-algebras. Consequently, we can append the classical input to the operator space under the tensor product via $\phi : L(H_B) \otimes C(X) \to L(H_A)$, where $C(X)$ is the space of continuous functions defined on the set X.

Some examples of quantum channels include states, observables, and a measure-and-prepare channel we now consider. Let us suppose that party A and party B wish to send information between them [9, 11, 12]. Party A measures an observable and sends the result to B classically. B then prepares their quantum system. In the Schrodinger perspective, the measure-and-prepare channel is given by the composition

$$\phi(\rho) = (\phi_2 \circ \phi_1)(\rho) = \sum_i \rho(F_i)R_i, \tag{3}$$

where F_i and R_i are both in the i-th quantum state and ϕ_1 and ϕ_2 denote the measurement and preparation maps, respectively.

4 Zero-Knowledge Proof

In cryptography, the zero-knowledge protocol is a method in which one party conveys to another party, some verifier, that they know some value without conveying any information apart from the fact that they have that value. The essence of zero-knowledge proof is to prove that one possesses such information without revealing the information itself or any additional information. These are done by trapdoor functions (like hash algorithms like SHA-256) [10] that can only be inverted by knowing the solution or searching the entirety of the domain, which is an NP-hard problem. However, using quantum algorithms, one could search the function's domain to effectively tamper or find out the original information in $O(n)$. On the other hand, if one were to attack a user in a blockchain application that transmits classical data into a quantum channel, they would find it difficult to copy data encoded in a quantum state [2]. This means that if one tried to observe or eavesdrop on the quantum state, the qubit state would be changed due to wave function collapse (no-cloning theorem), meaning that the server will be indicated if a user attempts to tamper with data.

We may prove that two people have the exact quantum representation of the data (near 0 chance of collisions and near 0 probability of someone finding a collision as qubits lose their coherence every time they are measured) if

$$\Pr(|\psi\rangle{=}1) - \Pr(|\psi'\rangle = 1) < \epsilon, \tag{4}$$

where $|\psi\rangle$ and $|\psi'\rangle$ represent two quantum states of two separately entered data sets, and ϵ is negligible.

In numerous large-scale blockchains, application servers use the existence hash trees or Merkle trees in which every leaf node is labeled with the cryptographic hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. The implementation is with the objective for storage optimization while also retaining the zero-knowledge proof that some data value exists [13]. We may similarly use the entanglement of qubit states (in a tree-like structure) to retain zero-knowledge proof to entangle the quantum representation of numerous data blocks while retaining information such as timestamp and identification information [5].

5 Experimental Results

In this research, we lacked access to a quantum computer and had an inability to transmit data through classical to quantum mapping, but we could simulate a post-quantum data transmission using pseudo-quantum signals. The steps used in a classical mapping to pseudo-quantum mapping are as follows.

We separate our raw data input into two raw arrays of qualitative and quantitative data to turn the associated quantitative data into a quantum/pseudo-quantum state. Using binary conversion tables, hexadecimal ASCII conversions, and other such methods we can numerically represent all of our data [7]. We can use a wavelet transform function on our numerical data to convert our numerical data into a pseudo-quantum signal using the equations

$$\alpha = \begin{bmatrix} -0.0674 \\ 0.0942 \\ 0.4058 \\ 0.5674 \\ 0.5674 \\ 0.4058 \\ 0.0942 \\ -0.0674 \end{bmatrix} \beta_1 = \begin{bmatrix} -0.0942 \\ 0.0674 \\ 0.5674 \\ 0.4058 \\ -0.4058 \\ -0.5674 \\ -0.0674 \\ 0.0942 \end{bmatrix} \beta_2 = \begin{bmatrix} -0.0942 \\ -0.0674 \\ 0.5674 \\ -0.4058 \\ -0.4058 \\ 0.5674 \\ -0.0674 \\ -0.0942 \end{bmatrix} \beta_3 = \begin{bmatrix} -0.0674 \\ -0.0942 \\ 0.4058 \\ -0.5674 \\ 0.5674 \\ -0.4058 \\ 0.0942 \\ 0.0674 \end{bmatrix} \tag{5}$$

$$WD = \begin{bmatrix} A \\ d_1 \\ d_2 \\ d_3 \end{bmatrix}, \theta_{ij} = \frac{\pi(A_{ij}) + \max(A_{ij}) - 2\min(A_{ij})}{6(\max(A_{ij}) - \min(A_{ij}))}, \tag{6}$$

where D represents our input data matrix, θ represents the pseudo-quantum signal of the data, and α, β_1,β_2, and β_3 are filter banks for our wavelet transform matrix W.

Classically, we implemented a simple peer-to-peer network by creating a centralized server and used socket programming to communicate from a client peer to all other peers via a centralized server. In our experiments, we first converted the data into a pseudo-quantum signal (represented by a NumPy array in python) which is then converted to a byte array for sending over a socket. Then, the byte array was converted back to the data's pseudo-quantum signal representation on the receiving side [7, 14].

6 Conclusions

In this research, we developed a security scheme to make a quantum computing-resistant cryptographic application. The security scheme we developed was the use of classical to quantum mappings for zero-knowledge proof of data. This proposed security scheme was done in accordance with finding a solution to Grover's algorithm's effect on hashing. In this research, we were able to mathematically and quantum mechanically prove the post-quantum nature of the qubit representations of classical data. We were also able to explore methods of data encryption and network storage using quantum mechanical properties. Classically, we used a pseudo-quantum representation to illustrate a peer-to-peer network that's able to send, receive, encode, and decode pseudo-quantum signals of classical data.

References

1. Vadhan SP (2017) The complexity of differential privacy. Tutorials Found Cryptogr. https://doi.org/10.1007/978-3-319-57048-8_7
2. Rodenburg B, Pappas SP (2017) Blockchain and quantum computing. MITRE
3. Diffie W, Hellman M (2021) New directions in cryptography (1976). Ideas That Created the Future, pp 421–440. https://doi.org/10.7551/mitpress/12274.003.0044
4. Chen L et al, Report on post-quantum cryptography. National Institute of Standards and Technology, NISTIR 8105. https://doi.org/10.6028/NIST.IR.8105
5. Grover LK (2001) From Schrdinger's equation to the quantum search algorithm. Pramana 56(2–3):333–348. https://doi.org/10.1007/s12043-001-0128-3
6. Weedbrook C, Pirandola S, Garca-Patrn R, Cerf Nicolas J, Ralph Timothy C, Shapiro Jeffrey H, Lloyd S (2012) Gaussian quantum information. Rev Mod Phys 84(2):621–669. arXiv:1110.3234
7. Lin T, Xu S, Shi Q, Hao P (2006) An algebraic construction of orthonormal M-band wavelets with perfect reconstruction. Appl Math Comput 172:717–730
8. Cortese JA, Braje TM (2018) Loading classical data into a quantum computer. arXiv:1803.01958v1 [quant-ph] 5 Mar 2018
9. Bernstein DJ, Buchmann J, Dahmen E (2009) Post-quantum cryptography. Springer, Berlin. https://doi.org/10.1007/978-3-540-88702-7
10. Grover LK, A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp 212–219. ACM. https://doi.org/10.1145/237814.237866, arXiv:quant-ph/9605043
11. Wilde MM (2017) Quantum information theory. Cambridge University Press, Cambridge. arXiv:1106.1445
12. Sun X, Sopek M, Wang Q, Kulicki P (2019) Towards quantum-secured permissioned blockchain: signature, consensus, and logic. Entropy 21(9):887. https://doi.org/10.3390/e21090887
13. Nielsen Michael A, Chuang Isaac L (2010) Quantum computation and quantum information: 10th, anniversary. Cambridge University Press, Cambridge. https://doi.org/10.1017/cbo9780511976667
14. Choi K (2019) Differentially private M-band wavelet-based mechanisms in machine learning environments

Balance Model of Ukraine's Gross Domestic Product Optimization on the National Economy Branches on the Basis of Information and Communication Technologies

Alina Yakymchuk, Mykola Shershun, Andriy Valyukh, and Taras Mykytyn

Abstract Increasing productivity of the economy branches determines the formation of the basis for achieving sustainable development for both states and individual territories. The aim of this investigation is a production processes optimizing of different economy sectors on the basis of a balance model, to develop international cooperation in the field of introduction of information–communication technologies between Ukraine and European Union. The authors examine the processes of Ukraine's industrial production activities and, in particular, on the level of some brunches of national economy. A set of measures for stimulating the provision of gross domestic product has been offered. Determined income per unit of gross output gives each of the industries in Ukraine. The next step is to set the required volume of gross output to obtain a unit of income.

Keywords European Integration Gross Domestic Product Economic Policy · Balance model

A. Yakymchuk (✉)
National University of Water and Environmental Engineering, Soborna, str. 11, Rivne 33028, Ukraine
e-mail: a.y.yakymchuk@nuwm.edu.ua; alinayakim@ukr.net

M. Shershun
Institute of Environmental Management and Agroecology, Ukraine's National Academy of Agrarian Sciences, Metrological Str., 12, Kyiv 03143, Ukraine
e-mail: shershun_mh@ukr.net

A. Valyukh
Open International University of Human Development «Ukraine», Kotlyarevskogo Str., 1c, Rivne 33028, Ukraine
e-mail: a.m.valyukh@ukr.net

T. Mykytyn
Rivne State Humanity University, Stepana Bandery Str., 12, Rivne 33028, Ukraine
e-mail: tapac_m@ukr.net

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_77

1 Introduction

Gross domestic product (GDP) has been the market value and total monetary value of all produced goods and services within a country's economy during a year. GDP is a generalized comprehensive indicator of the economic health of each individual country; it is a dynamic indicator of total domestic production. The economical development on the basis of information–communication technologies was highlighted in the works of [1–5] and others. But to date, a country's GDP will rising when prices tend to increase, but this does not always reflect any changes in the quality or quantity of goods and services, which were produced. That is why, it now can be difficult to research just an economy's nominal GDP in annual year, whether the figure has risen because prices rose or it is a real expansion in production. Economic growth requires businesses to attract new labor in various industries. That is why a country with a high GDP usually has a low unemployment rate. Economic development depends on many factors, one of which are the level of technology, communications, and management. There are many studies about the information–communication technologies' impact on GDP; but in the international context, the influence of ICT on GDP growth is insufficiently studied. In the world, some economies use technology transfer and thereby accelerate and revitalize their development, while others do not. The relationship between international technology transfer in EU and economic growth has investigated by different scientists [3, 6, 7]. So, the transfer technology has been complemented by national innovation capabilities based on innovative development and research. The digital technologies' ability has been unlocked by far being fully utilized. On the Research and Oxford Economics Accenture's estimation, the digital economy, which includes digital capital and digital skills, accounts for 22.5% of world GDP. Until now, nascent digital companies and technology giants have benefited from digital disruptions. But there is a good opportunity for traditional businessmen to apply new ICT and models of business more effectively [3, 5].

The article defines the advanced technical development strategies and examines how do they influence on economic development of the state and GDP; identified the relationship between ICT introduction and GDP growth on balance method for Ukraine; and identified external and internal tools for the economical and technology growth for Ukraine according to the European Union's directives.

2 Methodology

Methodological and theoretical basis of this investigation has been a fundamental provisions of economic theory. In this research, some general scientific methods were applied as systematization—to analyze economic condition and level of profitability of certain sectors of the economy of European countries and Ukraine; cause and consequences method—to study the influence of the economic crisis and pandemic COVID-2019. The following special methods were applied as balance modeling method—to calculate the matrix of revenues to the budget for each sector of the economy; benefits and costs analysis—to assess the economic efficiency on the implementation best foreign practices in optimization of Ukrainian enterprises; and imitation modeling—for quantitative assessment optimizing scenarios of the process of enterprise budgeting. To implement the process of optimizing the GDP of Ukraine in this paper, a balance model is developed, where the initial data are gross output (X), budget revenues (Y) by type of taxes from each of the industries. The calculation has been based on the optimization of revenues from each sector of the national economy and stimulating the production of GDP by these sectors.

3 Results and Discussion

Developed countries in recent years have attracted a significant amount of ICT. USA have optimized in investments in digital skills, digital technologies, and ICT; this country increased its GDP by 2,1%, or to US $ 421 billion only during 2020 year. The ICT now can influence on productivity growth; it has the features of knowledge capital, both through capital deepening and its spillover effects. Now, smarter use of digital could boost productivity and generate per year additional economic output near US $2 trillion. So, ICT can act as a growth multiplier in the future few years. Understanding where to make those investments to realize the real improvement in gross domestic product is the subject of last analysis by Strategy and Oxford Economics Accenture [8]. Due to IKT technology, policy makers and business leaders can be more productive, competitive, and bring for people better life quality.

There are real and nominal GDP. If there is a noticeable difference between the countries' real and nominal GDP, it can be a clear indication of significant deflation or inflation in the economy of the state. Based on GDP price, deflator can be calculated real GDP, which has been the difference in prices between the current and last years. Nominal GDP consists of deflator and yielding real GDP. Real GDP is mainly lower than nominal one because inflation is typically a positive number. Real GDP affects changes in market value, and this narrows the difference between year-on-year outputs.

To implement the optimization process, the authors made a balance model, where the initial data are gross output (X), budget revenues (Y) by type of taxes from each of the industries (Table 1). It is a comparative assessment of economic factors impact on the development of ICT, forecasting amount of funding with the optimal value of implemented country's ICT.

Based on the initial data, we calculate the matrix of budget revenues for each industry. This matrix looks like this:

Table 1 Initial data of balance model of gross output, budget revenues, and type of taxes from each of the industries

Branches	Tax for profit, million UAH	Land fee, UAH million	Profitable personal income tax, UAH million	Tax on vehicle owners, UAH million	Local taxes, million UAH	Budget revenues, UAH million (Y)	GDP, million UAN (X)
Electricity	1.59181	0.49401	1.9212	0.2745	0.6038	5.489	45.003
Chemical Industry	9.40615	2.91915	11.352	1.6218	3.5679	32.435	281.3339
Engineering	1.30239	0.40419	1.5719	0.2246	0.494	4.491	25.59
Light industry	0.72355	0.22455	0.8733	0.1248	0.2745	2.495	6.66
Woodworking industry	0.28942	0.08982	0.3493	0.0499	0.1098	0.998	2.22
Food industry	1.15768	0.35928	1.3972	0.1996	0.4391	3.992	51.83

Source Calculated based on the [1, 4, 8–11]

$$A = \begin{vmatrix} 0.0354 & 0.0110 & 0.0427 & 0.0061 & 0.0134 \\ 0.0334 & 0.0104 & 0.0403 & 0.0058 & 0.0127 \\ 0.0509 & 0.0158 & 0.0614 & 0.0088 & 0.0193 \\ 0.1086 & 0.0337 & 0.1311 & 0.0187 & 0.0412 \\ 0.1304 & 0.0405 & 0.1573 & 0.0225 & 0.0495 \\ 0.00223 & 0.0069 & 0.0270 & 0.0039 & 0.0085 \end{vmatrix}$$

We form a matrix (1-A):

$$A = \begin{vmatrix} 0.9646 & -0.0110 & 0.0427 & -0.0061 & -0.0134 \\ -0.0334 & 0.9896 & 0.0403 & 0.0058 & 0.0127 \\ 0.0509 & -0.0158 & 0.9386 & -0.0088 & -0.0193 \\ -0.1086 & -0.0337 & -0.1311 & 0.9813 & -0.0412 \\ -0.1304 & -0.0405 & -0.1573 & -0.0225 & 0.9505 \\ -0.0223 & -0.0069 & -0.0270 & -0.0039 & 0.9915 \end{vmatrix}$$

We determine what income per unit of gross output produces each of the industries:

$$\begin{vmatrix} y1 = 0.8780 \\ y2 = 0.8847 \\ y3 = 0.8245 \\ y4 = 0.6254 \\ y5 = 0.5505 \\ y6 = 0.9230 \end{vmatrix}$$

To set the required output of gross output to obtain a unit of income, we use the formula: Y = (1 – A) * X:

$$Y = \begin{vmatrix} 1.0433 & 0.0134 & 0.0523 & 0.0075 & 0.0164 \\ 0.0410 & 0.0127 & 0.0494 & 0.0071 & 0.0155 \\ 0.0624 & 0.0194 & 1.0753 & 0.0108 & 0.0237 \\ 0.1331 & 0.0413 & 0.1606 & 0.0229 & 0.0505 \\ 0.1597 & 0.0496 & 0.0229 & 0.0275 & 0.0606 \\ 0.0274 & 0.0085 & 0.0330 & 0.0047 & 0.0104 \end{vmatrix} * \begin{vmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{vmatrix} = \begin{vmatrix} 1.1494 \\ 1.1412 \\ 1.2150 \\ 1.4590 \\ 1.5508 \\ 1.0944 \end{vmatrix}$$

Table 2 presents the balance sheet model. To generate revenue in the electricity sector of UAH 1 million, it is necessary to increase GDP by UAH 1,1494 million, and income tax revenues will increase by UAH 23,8 thousand, land fees—by 3,5 thousand. UAH, tax on vehicle owners—by 4,5 thousand UAH, water fee—by 5,9 thousand UAH, local taxes will increase by 6,8 thousand UAH, other revenues—by 2,3 thousand UAH; to generate revenue of UAH 1 million, in the chemical industry, it is necessary to increase the volume of production to UAH 1,044 million, in mechanical engineering—to UAH 1,063 million, in light industry—to UAH 1092 million, in the woodworking industry—up to an approximate output of UAH 1,1 million, and in the food industry—up to UAH 1,03 million in accordance. To increase the revenue side of the budget from industry to the level of UAH 225 million, it is necessary to increase GDP in the electricity sector from 883 to 896.18, in the chemical industry to UAH 296,5 million, in mechanical engineering—to 78,75. UAH million, in light industry—up to UAH 47,1 million, in woodworking—up to UAH 101,1 million, and in the food industry—to the level of UAH 229,3 million. Thus, the additional gross output will amount to UAH 76,93 million.

Table 2 Estimated balance model

Branches	Tax for profit, million UAH	Land fee, UAH million	Profitable personal income tax, UAH million	Tax on vehicle owners, UAH million	Local taxes, million UAH	Budget revenues, UAH million (Y)	GDP, million UAN (X)
Electricity	0.0354	0.0334	0.0509	0.1086	0.1527	1	1.1494
Chemical Industry	0.0110	0.0104	0.0158	0.0337	0.0474	1	1.1412
Engineering	0.0427	0.0403	0.0614	0.1311	0.1573	1	1.2150
Light industry	0.0061	0.0058	0.0088	0.0187	0.0264	1	1.4590
Woodworking industry	0.0134	0.0127	0.0193	0.0412	0.0580	1	1.5508
Food industry	0.0134	0.0127	0.0193	0.0412	0.0580	1	1.0944

Source Calculated based on the [1, 2, 4, 11]

GDP is often viewed as an indicator of the population living standards, as in some cases it is used for this purpose due to the lack of more suitable indicators. However, the use of GDP as an indicator of the well-being of the population is, in a sense, a compromise solution associated with the absence in practice of other internationally comparable indicators of income and well-being. That is why high-tech economies could benefit more from the optimal combination of investment in new cutting-edge technologies, digital skills, and ICT. Taking into account that in the EU not all countries are developing at the same speed, in some member states, the ICT employment rate is higher while in other countries, it is lower. Another yardstick to see whether gross domestic product is increasing is wage of the people compare to last year's. If the country or economy is in recession, then the GDP will be decreasing. The demographic situation, economical factors, development index, education level, and literacy rate are only a few of the factors that contribute to the employment rate overall, including in the ICT sector [12]. Netherlands, Luxembourg, Ireland, and Estonia are on the 3–6 positions when it comes to the general share of ICT specialists compared to their national workforce. At the end of the list, there are Cyprus (3,1%) Romania (2,5%), and Greece (2%).

Gross domestic product is the most frequently used measure for the estimation of overall size of an economy of the state or to monitor economic convergence or divergence within the EU countries. GDP per capita has been widely used indicator for determination of living standards. The Development Indicators database of World Bank, based on data from national statistical institutes and international organizations, is used as a source of information on the size of the GDP of countries and territories of the world. In combination with other indicators of GDP, it is used to characterize various aspects of the economic process as well as to analyze fluctuations in the economic environment. The EU has a major role to play in the development of ICT by creating meeting points between productive industries, applied research, and varieties of technology. Large companies today are the main consumers of complex financial products, because they are focused on the main production, and they transfer responsibility for managing accounting risks for various insurance and financial institutions. Business and policy managers must invest heavily in the required areas; thanks to this, they can help their economy grow.

4 Conclusions

The European Union has an important positive experience of ICT implementation for Ukraine's economy. In the process of globalization, companies have increased risks; this is an indisputable fact. Moreover, these risks can be financial, technological, and industrial, even reputational, and so on. That is why companies increasingly need to use financial and insurance services to protect their activities. The increasing complexity of the technologies used for ICT, calling on extremely diverse skills, has placed ICT at the heart of present industrial dynamism. The ICT employment rate in the EU reached 4.3% in 2020 from 3.9% in 2019. One of the key players that lead to the ICT employment growth in the EU is the pandemic. In the EU, younger generations have a high interest in the digitalization process too.

To stimulate the development of regional Ukraine's ICT, it is necessary to introduce the best practices of foreign experts, scientists, cluster professionals, and people who make managerial and economic decisions. Best international experience shows us that financing in the early (preliminary and initial) stages of an economic and ICT project should be in the form of grants or equity financing and not in the form of repayment. The process of assessing the impact of group interventions on methodological design and finding economic tools for innovation should be realistic and provided for in advance in territorial development programs and in the relevant budgets. In this regard, grants from the European Union are extremely important for the development of information and communication technologies in Ukraine. It is the grant funds and co-financing in projects that are the donor of financial resources for the development of ICT in Ukraine.

The authors formed a balance model, which showed that a number of actions it is necessary to increase the gross national product in Ukraine. In particular, today it is necessary to generate revenue in the electricity sector to increase GDP by UAH 1,1494 million per capita, and will increase income tax revenues and land fees, tax on vehicle owners, water fee, local taxes will increase. To generate revenue of UAH 1 million, in the chemical industry, it is necessary to increase the volume of production, in mechanical engineering, in light industry, in the woodworking industry—up to an approximate output of UAH 1,1 million, and in the food industry—up to UAH 1,03 million in accordance. To increase the revenue side of the budget from industry to the level of UAH 225 million, it is necessary to increase GDP in the electricity sector, in the chemical industry, in mechanical engineering, in light industry, in woodworking, and in the food industry; thus, the additional gross output will amount to UAH 76.93 million.

The establishment of European ICT centers in the regions of Ukraine would create the necessary consultation and economic conditions for cooperation throughout Europe and Ukraine in the field of key joint programs and the development of industry and ICT processes in peripheral territories. All these measures will significantly improve both the economic and environmental situation in Ukraine. Most importantly, Ukraine need to develop the ICT process not as a ready-made formula, but as a tool to facilitate adaptation to any favorable or not favorable conditions, sectors of the economy, and the country in the framework of cooperation, which is well coordinated and decentralized.

References

1. Organisation for Economic Co-operation and Development (OECD). OECD Data: Gross National Income [URL: data.oecd.org]
2. Organisation for Economic Co-operation and Development (OECD). Gross National Income (GNI) Indicator [doi:https://doi.org/10.1787/8a36773a-en].
3. Baldwin M (2006) The euro's trade effects. Working paper series ECB, № 594

4. State Statistics Service of Ukraine (2019). http://www.ukrstat.gov.ua
5. Dedrick J, Gurbaxani V, Kraemer KL (2003) Information technology and economic performance: a critical review of the empirical evidence. Center for Research on Information Technology and Organizations, University of California, Irvine
6. Vasyltsiv T et al (2020) Economy's innovative technological competitiveness: decomposition, methodics of analysis and priorities of public policy. Manag Sci Lett 10(13):3173–3182
7. Dickey DA, Fuller WA (1981) Likelihood ratio statistics for autoregressive time series with a unit root. Econometrica 49:1057–1072
8. Digital disruption: The growth multiplier (oxfordeconomics.com)
9. The World Bank. World Development Indicators Database: Gross Domestic Product [URL: data.worldbank.org]
10. International Monetary Fund (IMF). World Economic Outlook Database: Gross Domestic Product [URL: imf.org/en/Data]
11. International Monetary Fund (IMF). World Economic Outlook [URL: imf.org/en/Publications/WEO]
12. The ICT Employment Rate in The European Union (techbehemoths.com)
13. Aglietta M (2012) Zone euro, éclatement ou fédération, Michalon
14. Yakymchuk A et al (2020) Public administration and economic aspects of Ukraine's nature conservation in comparison with Poland. In: Kantola J, Nazir S, Salminen V (eds) Advances in human factors, business management and leadership. AHFE 2020. Advances in intelligent systems and computing, vol 1209. Springer, Cham
15. Ciborowski R, Skrodzka I (2019) International technology transfer as innovation factor in EU countries. https://www.inderscience.com/info/inarticle.php?artid=81708
16. Mykytyn T, Yakymchuk A, Valyukh A (2017) Management of protected areas of Ukraine's Polissia: international experience. Probl Perspect Manag 15(1):183–190
17. Coppell J (2002) E-commerce: impacts and policy challenges. OECD, Working Papers, NO. 252, June 2002
18. Engle RE, Granger CWJ (1981) Cointegration and error-correction: representation, estimation and testing. Econometrica 55:251–276
19. Granger C, Newbold P (1974) Spurious regressions in econometrics. J Econometrics 2:111–120
20. Johansen S, Juselius K (1990) Maximum likelihood estimation and inferences on cointegration with approach. Oxford Bull Econ Stat 52:169–209
21. Nelson CR, Plosser CI (1982) Trends and random walks in macroeconomic time series some evidence and implications. J Monet Econ 10:139–162
22. National accounts and GDP - Statistics Explained (europa.eu)

Identify and Classify CORN Leaf Diseases Using a Deep Neural Network Architecture

Naresh Kumar Trivedi, Shikha Maheshwari, Abhineet Anand, Ajay Kumar, and Vijay Singh Rathor

Abstract Disease attacks on vegetable plants must be anticipated and treated promptly to avoid yield loss. The majority of diseases that affect vegetable plants manifest themselves in their leaves or stems. Disease classification using leaf images is now possible due to advancements in deep learning algorithms. The primary objective is to design a system based on deep learning for the prediction and categorization of vegetable leaf disease. Corn vegetable crops are considered in this work. A publicly available dataset was used for training and testing. Convolutional neural network Inception V3 utilized to develop and test the system. As a result, the performance of the system is projected to be at its most significant level.

Keywords Deep learning · Inception V3 Image classification · Neural network

1 Introduction

Because India is primarily an agricultural country, agriculture plays a significant role in the Indian economy. As many as 70% of the rural population derive their principal income from agriculture. However, yields have decreased in the wake of the most recent disease outbreaks, and enormous economic losses have occurred. As a result, a prediction system is required to spot disease attacks and define the type of infection they cause, allowing farmers to take the necessary countermeasures. Corn, the primary food grain plant, was considered for this effort [1]. Three types of diseases are frequently found on maize plant varieties: Cercospora Gray leaf spot, Northern Leaf Blight, and common rust are all examples of these diseases. Although these attacks are visible on the leaf surface, untrained farmers may have difficulty

N. K. Trivedi · A. Anand (✉) · A. Kumar
Chitkara University Institute of Engineering and Technology, Punjab, India
e-mail: abhineet.anand@chitkara.edu.in

S. Maheshwari
Manipal University, Jaipur, India

V. S. Rathor
IIS (Deemed to Be) University, Jaipur, India

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_78

identifying them. Thus, developing an automated technique for detecting this type of disease assault will benefit farmers greatly [2].

Numerous complex forms of farming technology are designed to operate indefinitely and require human involvement or constant monitoring to avoid mechanical failures or errors. While the devices are expensive, their application range and usability are limited; expanding workflow requires further setup or progression. Smart farming collects data from real-time fields and analyses and forecasts it using advanced processing technology [3]. Significant effort has been made in the agriculture industry to develop revolutionary farming solutions based on deep learning tools. The advances of deep learning in a previous couple of years have been very remarkable. These new tools make it possible to obtain informative feature depictions from an almost unlimited amount of input photographs. Deep learning models will help growers improve their crop predictions and prevent financial losses. A single input layer, an output layer with multiple convolutional layers inside, is present in this neural network. To mimic the human brain, the model will include numerous hidden layers and neurons. Image-related tasks will see significantly increased accuracy because the situation is rich with learnable variables. The CNN algorithms Inception V3, Squeeze Net were employed in this paper [4, 5].

The following sections comprise the paper: Section 2 offers references to prior work, while Sect. 3 discusses the methods presented. The experimental data are examined in Sect. 4, and the conclusion is presented in Sect. 5.

2 Related Work

To begin identifying and classifying plant diseases, to correctly identify a plant species, one must know its family and species first. In this paper author used color-related attributes like mean, median, standard deviation, co-occurrence of Gray levels, lacunarity, and Shen features. Furthermore, author used a Bayesian classification model to classify the images [6]. On the other hand, proposed a method for detecting plant disease that incorporates the HSV feature and a support vector machine. Additionally, they developed a model for disease detection based on neural networks and optimized the loss function using a Genetic Algorithm and SVM [7, 8].

Author has compiled a paper on using multiple neural network models for diagnosing and classifying illnesses in leaf photographs. They introduced a variety of hyperspectral models, types, and classifiers using hyperspectral images as input [9].

The author discussed various classification methods for citrus leaf disease, including image processing techniques and their associated benefits, drawbacks, and obstacles [9].

A multilayer CNN classifier for identifying Anthracnose-infected mango leaves was proposed. The findings of this study used the CNN model to differentiate between a mangos leaves affected with a fungal illness [10].

To classify four cucumber diseases: leaf spots, powdery mildew, anthracnose, and downy mildew. Authors constructed a deep convolutional neural network model using a design from the literature.

Authors devised a technique for forecasting Powdery mildew and achieved 90 percent classification accuracy for Tomato spotted wilt virus in greenhouse bell peppers [11].

The authors recommended using pattern recognition to identify and classify three important diseases that affect cotton plants, specifically Alternaria, Bacterial Blight, and Myrothecium, The active counter model is used to extract the features, and Hu's moment is calculated. We photographed the Institute of Cotton Research in Nagpur and cotton crops in the Buldana and Wardha regions. This approach makes predictions with an accuracy of 85% [1, 12].

We found that most of the researcher used small data set and their accuracy level is significantly low. We will be using larger data set and try to enhance accuracy level with our proposed method.

Proposed Methodology

Using the Kaggle dataset, the algorithm receives input as photos (Fig. 1).

Kaggle is a publicly available dataset that contains 7316 photos of various illness types. For this undertaking.

Step 1: Extract pertinent photos from the Kaggle dataset.

Step 2 Classify the photographs depending on the diseases and label the classes accordingly.

Step 3: Before you begin processing the photographs, make use of an image embedded. For example, uploading a picture from a remote server to Image Embedder reads the Image and places it on the server. (Inception V3). Each image is assigned a feature vector using deep learning algorithms.

Step 4: Train the CNN with multiple architectures on the training dataset.

Step 5: Two different sets of validation data, Kaggle data sets, should be used to evaluate CNN designs.

Totally 7316 images were used in this work.

Description of the Dataset

See Table 1.

3 Methodology

CNN's are good for image categorization because of their use in deep learning. However, to learn correctly, CNN must be taught with a massive amount of data. Artificial intelligence computing of this form is designed specifically for picture classification. With machine learning approaches, the user must extract the feature and give it to the network. On the other hand, the user will only have to remove the feature with this algorithm. A CNN is a multi-leveled architecture that is built using many sequentially ordered layers. In this research, two distinct CNN architectures are compared. Each model starts with a relu activation function in the convolutional layer and finishes with a softmax activation function in the dense layer. f(a) = max (0, a) denotes the relu activation function, whereas f(ai) = k (eai / eak) denotes the softmax activation function. Every layer has a set number of adjustable parameters, defined in advance with ((width of the filter * height of the filter * previous layer + 1's number of filters)* number of filters).

Cross-validation (k fold) is a technique for determining the quality of a machine learning model using previously unseen data. They first utilized a small sample to explore its performance on all available data to evaluate the model's performance. They took advantage of this new information to utilize it to forecast data that was not part of the training process.

Cross-validation groups the data into approximately equal-sized groups and uses the groups to test different hypotheses. When the algorithm is being fitted, the k-1 remaining folds serve as validation sets.

3.1 Inception V3

Inception V3 is primarily concerned with conserving computational power through modifications to prior Inception architectures. This concept was advanced in the 2015 publication rethinking the Inception architecture for Computer Vision, and inventors collaborated on it.

Though Inception networks (Google's GoogLeNet and the first version of Inception) have fewer parameters and a lower computational cost, GoogLeNet and Inception are more efficient in terms of the number of parameters and cost (memory and other resources). Therefore, changes should be made to an Inception network carefully because its computational advantages must not be sacrificed. As a result, using an Inception network for different applications becomes difficult because the new network's efficiency is unknown.

One way to loosen the limitations of an Inception V3 model is to implement multiple optimization algorithms. These different techniques are incorporated in Factorized Convolution, Parallel Processing, Regularization, and Dimensionality Reduction [13, 14].

Inception V3 architecture is designed progressively, as described below:

1. Factorized Convolution: This significantly minimizes the model parameters required for computation. Additionally, it measures network efficiency.
2. In particular, replacing more extensive convolutions with smaller ones results in significant acceleration. For example, by removing the 5 5 filters and replacing them with two 3 3 filters, only 18 (3 * 3 + 3 * 3) parameters are required (when comparing the number of parameters needed for 3 3 filters and a 5 5 filter).
3. Thirteen convolution followed by a 31 convolution can be used instead of a 33 convolution. However, using a 33 convolution for a 22 one increases the number of parameters. In the middle layer, the three convolutions are connected, whereas

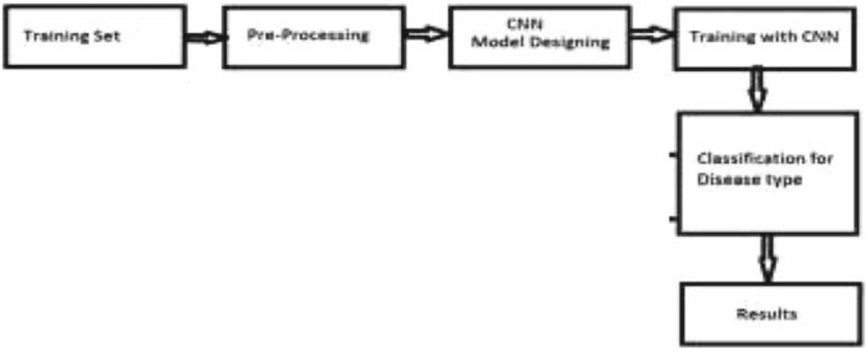


Fig. 1 Proposed work's overall architecture

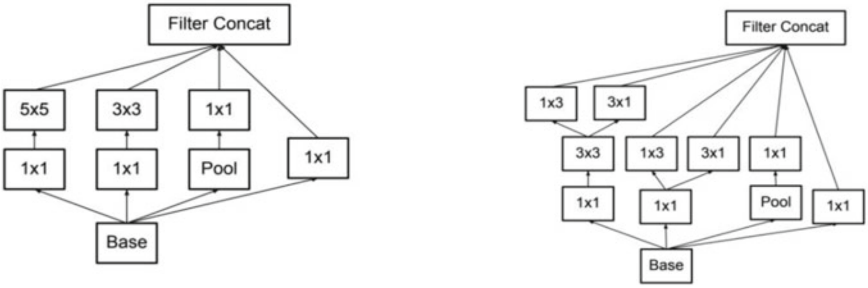


Fig. 2 Filter application in Inception V3 architecture

they are all connected in the bottom layer. They can also minimize the number of computations because they can share the weights of the 3 × 3 convolutions, can be seen in Fig. 2.

4. An auxiliary classifier is a little CNN that is inserted between layers of the neural network during training. This network's loss is added to the leading network's failure. To develop a deeper network, GoogLeNet employed additional classifiers, which are different. Inception V3 also uses auxiliary classifiers.
5. Pooling can be used to decrease the size of the grid. A more efficient computing technique is proposed [15].

4 Result and Analysis

Tables 2, 3 and 4 shows the number of leaves correctly classified by neural network with 5, 10, and 20 k fold values. Figure 3 show the scatter plot of classification accuracy with 5, 10, and 20 k fold.Comparison Table 5 clearly shows that the highest

Table 1 Dataset description

Corn disease type	Count of Kaggle dataset images	Images from fields and Google
Healthy	1859	548
Common rust	1907	236
Northern leaf blight	1908	37
Leaf spot	1642	434
Total images	7316	5941

Table 2 For k fold = 5

	Leaf spot Gray leaf spot Cercospora	Common rust	Leaf Blight Northern	Healthy	$\sum$
leaf spot Gray leaf spot Cercospora	1530	1	107	45	1642
Common rust	1	1902	4	0	1907
Leaf Blight Northern	45	3	1856	4	1908
Healthy	1	0	0	1858	1859
$\sum$	1569	1907	1974	1866	7316

Table 3 For k fold = 10

	Leaf spot Gray leaf spot Cercospora	Common rust	Leaf Blight Northern	Healthy	$\sum$
leaf spot Gray leaf spot Cercospora	1534	1	105	2	1642
Common rust	1	1903	3	0	1907
Leaf Blight Northern	41	1	1863	3	1908
Healthy	0	0	0	1859	1859
$\sum$	1569	1907	1974	1866	7316

classification accuracy 97.8% is achieved with k fold 20. All study is conducted utilizing Repeat Train/Test 10 and a 66% training set.

5 Conclusion

Convolutional neural networks have made remarkable strides in image processing and picture applications, thereby rekindling academics' excitement for ANNs. Numerous improvements are currently being made to enhance performance of such applications

Table 4 For k fold = 20

	Leaf spot Gray leaf spot Cercospora	Common rust	Leaf Blight Northern	Healthy	∑
leaf spot Gray leaf spot Cercospora	1537	1	101	3	1642
Common rust	3	1902	2	0	1907
Leaf Blight Northern	43	1	1861	3	1908
Healthy	2	0	0	1857	1859
∑	1569	1907	1974	1866	7316

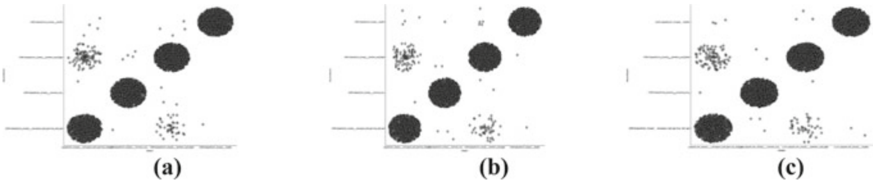


Fig. 3 Scatter plot **a** with k fold 5, **b** with k fold 10 and **c** with k fold 20

Table 5 Comparison for classification accuracy

Number of folds	AUC	Classification accuracy	F1	Precision	Recall
5	0.9983	0.9767	0.9767	0.9769	0.9767
10	0.9985	0.9785	0.9785	0.9787	0.9785
20	0.9985	0.9782	0.9782	0.9784	0.9782

by using CNN's, and this paper utilizes major Inception V3 CNN network to categorize leaf diseases. We chose Corn vegetable species with their corresponding leaf disease for this study. The network used in this paper is predicting with 98 percent accuracy. The experimental results indicate that increasing the number of layers and adding original data to incoming layers, such as Inception V3, can enhance prediction accuracy. As a result, the networks perform better with the available data. The prediction precision of real-time data can be addressed and enhanced in the future by implementing appropriate preprocessing procedures.

References

1. LeCun Y, Bottou L, Bengio Y, Haffner P (1998) Gradient-based learning applied to document recognition. Proc IEEE 86(11):2278–2324
2. Krizhevsky A, Sutskever I, Hinton GE (2012) ImageNet classification with deep convolutional neural networks. Adv Neural Inf Process Syst 25 (NIPS):4824–4833

3. Simonyan K, Zisserman A (2014) Very deep convolutional networks for large-scale image recognition. arXiv preprint
4. He K, Zhang X, Ren S, Sun J (2016) Deep residual learning for image recognition. In: IEEE conference on computer vision and pattern recognition (CVPR), 1063–6919
5. Schor N, Bechar A, Ignat T, Dombrovsky A, Elad Y, Berman S (2015) Robotic disease detection in greenhouses: combined detection of powdery mildew and tomato spotted wilt virus. IEEE Rob Autom Lett
6. Kadir A (2014) A model of plant identification system using GLCM, Lacunarity and Shen features. Res J Pharm Biol Chem Sci 5(2)
7. Naik MR, Sivappagari C (2016) Plant leaf and disease detection by using HSV features and SVM. IJESC 6(12)
8. Trivedi NK, Kumar S, Jain S, Maheshwari S (2021) KFCM-based direct marketing. In: Rathore VS, Dey N, Piuri V, Babo R, Polkowski Z, Tavares JMRS (eds) Rising threats in expert applications and solutions. Advances in intelligent systems and computing, vol 1187. Springer, Singapore. https://doi.org/10.1007/978-981-15-6014-9_57
9. Golhsani K, Balasundram SK, Vadamalai G, Pradhan B (2018) A review of neural networks in plant disease detection using hyperspectral data. Inf Process Agricult 5:354–371. https://doi.org/10.1016/j.inpa.2018.05.002
10. Iqbal Z et al (2018) An automated detection and classification of citrus plant diseases using image processing techniques: a review. Comput Electron Agricult 153:12–32. https://doi.org/10.1016/j.compag.2018.07.032
11. Pratap Singh U, Chouhan SS, Jain S, Jain S (2019) Multilayer convolution neural network for the classification of mango leaves infected by anthracnose disease. IEEE Access 7(43721–43729)
12. Ma J, Du K, Zheng F, Zhang L, Gong Z, Sun Z (2018) A recognition method for cucumber diseases using leaf symptom images based on deep convolutional neural network. Comput Electron Agricult 154:18–24. https://doi.org/10.1016/j.compag.2018.08.048
13. Rothe PR, Kshirsagar RV (2015, January) Cotton leaf disease identification using pattern recognition techniques. In: 2015 international conference on pervasive computing (ICPC), pp 1–6. IEEE
14. Priya S, Uthra RA (2020) Comprehensive analysis for class imbalance data with concept drift using ensemble based classification. J Ambient Intell Humanized Comput
15. Szegedy C, Ioffe S, Vanhoucke V, Alemi AA (2017, February) Inception-v4, inception-resnet and the impact of residual connections on learning. In: Thirty-first AAAI conference on artificial intelligence

Consideration for NoSQL Databases Technical Consolidation

Abhijeet Singh Bais and Navneet Sharma

Abstract In the era of business analytics, enterprises are processing and persisting data from a variety of sources. Data sources include structured, unstructured, and semi-structured. Some data sources are schema driven and many are schema-agnostic. NoSQL databases serve the need of persisting, processing, and managing unstructured as well as structured data in different ways. It is important to select the right set of NoSQL for analytics-driven organizations. In the paper, the intention is to determine guidelines and consideration that can help enterprises to select the right set of NoSQL and consolidate NoSQL technologies for optimization. The right combination of NoSQL databases can help homogeneous technology footprint along with cost benefits & effort benefits for an analytics-driven enterprise. Design principals to help select between graph databases, document databases, and in-memory databases and in memory.

Keywords NoSQL · Key-value stores · Column stores · Document stores · Graph stores · Unstructured · Structured data storage

1 Introduction

Organizations are facing more and more challenges while handling data which includes the various process of data management like collecting, searching, retrieving, persisting, and querying. The main challenge is the data format. NoSQL databases are entirely different from relational tables and non-tabular; NoSQL databases are classified based on their data model designs such as key-value, document, column, and graph [1].

The NoSQL be a contemporary approach for the novel storage methods and with various benefits [2], like flexibility, scalability, and high loads.

A. S. Bais (✉) · N. Sharma
Department of CS & IT, IIS (Deemed To Be University), Jaipur, India
e-mail: abhijeetbais@gmail.com

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_79

2 Literature Review

1. Charles C Tappert and Hilda Mackin, Gonzalo Perez (2016)—They identified possible known risks of choosing NoSQL database and with actual risks computing quality measurements, which are critical while selecting the right NoSQL database for a business domain
2. A. Rafique, D. Van Landuyt, B. Lagaisse and W. Joosen (2018)—An in-depth study conducted by them. They compared various NoSQL platforms for data access. According to them, diversified and faster adoption of this NoSQL will become useful for the data industry.
3. Wade L SchulzMD, G. Nelson, Donn K. Felker, Thomas J.S Durant, Richard Torres (2016)—They compared RDBMS with NoSQL databases on the basis of storage, indexing, and query efficiency. Their findings strongly supporting the use of novel database technologies.
4. Aqel M. J, Al-Sakran A, Hunaity M. A (2019)—Their viewpoint is that NoSQL databases may be a suitable option for many applications, but it is difficult to fully replace relational database systems (RDBMS). Further, they conducted a survey to determine better and suitable database for the use case. In their paper, they discussed and compared the usage of Cassandra, HBase, and CouchDB.
5. Plechawska-Wojcik, Malgorzata & Rykowski, Damian. (2016)—They studied a set of social media websites and use cases by using different data store for each use case. Investigation was performed to determine operational performance parameters as well as data models. This study took place of three different type of relational, document, and graph databases.
6. Tang, E., & Fan, Y. (2016)—In this paper, base properties were discussed and evaluated the performance of NoSQL clusters.
7. Kumar, K. B. S., Srividya, & Mohanavalli, S. (2017)—This study was conducted on an online system which was streaming dataset on real time. There were various attributes including execution time of two popular NoSQL databases which were considered for the study.
8. Morais, Diogo Augusto Pereira & Edison Pignaton de Freitas (2017)—This paper concluded that Couchbase database has better execution time as well consistency while using multi-threaded process. The conclusion was drawn based on comparing three popular NoSQL data stores. Multiple iterations were performed to compare performance of these databases for the given use cases.
9. Naheman, W. & Jianxin Wei. (2013)—This paper explains shortfalls of relational databases and various advantages of NoSQL data stores. This paper also outlines common disadvantages using NoSQL databases. This study includes architecture for one of the column family databases, i.e., Hbase.

3 RDBMS or NoSQL

Understanding ACID vs BASE properties shall help to determine the need of NoSQL or RDBMS or already being used in your organization which will suffice [3].

3.1 Need of NoSQL Databases and Limitation of Relational Databases

Scaling has been a challenge for relational databases. Major constraint is maintaining referential integrity for a large dataset [4]. CAP theorem explains key factors needed for a distributed database system, which are:

- C-Consistency
- A-Availability
- P-Partition tolerance.

Scalability is difficult to achieve in the RDBMS.

Scalability and execution time are reciprocal to each other. There are some NoSQL databases which are explained based upon query performance for the same set of data with following:

- Light weight processing or low resource utilization
- Faster performance.

Key-Value Database. A pair of key and value is stored in an array collection of arrays which is stored and is like map. Each key is paired with only one value in the collection. This arrangement is known as key-value pair.

- Key-value pair is persisted as string value, which is like Hash. Value retrieval can be executed based on keys.
- Each key has one associated value which is of blob data type.
- Key-value storage limits way of accessing data. SQLs or other query languages do not support. All ACID operations can be performed using various commands.
- Key-value datasets support selecting, sorting, and updating, deleting commands. Query output is stored in the object format in memory [5].

Here are some popular key-value store databases: Riak, Memcached, Cassandra, Couchbase Server, Aerospike, Redis.

Riak is open-source database which uses multiple nodes to process the distributed data processing, whereas as Memcached is a distributed in-memory database. In--memory processing may have risk of data loss but it will be quicker in data processing, persistent data processing will have less or no risk of data loss, and processing may have slower performance than in-memory processing. There are multiple scalable NoSQL key-value stores, and to select suitable key-value store, need to be considered upon.

Access pattern—Query on the key.

Data Model—key-value collection data persistence and data storage as blob containers.

Scalability—Data distribution between servers is depending on keys. Certain range of data will be stored at node one and next range of keys will be stored at another node, once node is down range of data keys stored on that will be lost.

Distribution—Key and its value need to store in the same location which involves data replication a complex process while writing.

Uses of Key-Value Store. There is many common applicability for key-value stores such as,

- Web application session storing
- Shopping website checkout information.

Example: In a shopping website, information of the product is stored where each product is given a key generally called as product code. While checking out the product, then a particular product is accessed based on that key. In physical stores keys are printed as barcode to retrieve product related specification including price and discounts etc. Website shopping transaction steps.

- Retrieve product details bases on the key, in this case product code.
- Addition of a new product to the catalogue, allocate a product code as key and store product details as value before writing as key-value pair.
- While checkout, you can retrieve multiple product details for selected product codes. Which are Keys in the data store.
- Delete the product for a product key/code.

Document Database. Similar to key-value data stores, document databases are also collection of documents. And, each document contains key-value pair in the form of BSON /XML/ JSON.

- Generally, each document is tagged with an identifier so that indexing can be simplified
- All ACID transactions can be performed.
- Ability to store data in json/xml documents makes a good choice for complex data storage solutions.
- Document databases do not support relations like foreign key or referential integrity. Every document in the collection is exclusive.
- Similar to relations, joins are also not supported by document NoSqls.

Here are some popular the document databases: MongoDB, MarkLogic,CouchDB, OrientDB, RavenDB.

Access Pattern—Query on the key.

Operations—Only single document transactions are supported by document stores.

Data Model—Unlike relational model, it is schema free data model, and each document in the collection can store different number of key and different number of columns. It does not need schema.

Scalability—Document is an independent entity which contains complete data including relations in it. Sharing documents to different nodes is easy [6].

Column family Database. Set of columns call family of columns and row get stored for the family [7]. Each row can have different number of columns. Mainly, this is the group of similar or related data that can be accessed together.

- It is like the RDBMS table.
- Data stored as rows and columns can be added to rows any time. Each row may have different set of columns.

Popular column family data stores are—Hbase, Hypertable, Amazon DynamoDB. Hbase is the one of the best column family databases with write operations [8].

Highlights of Column Family Data store.

Access Pattern—MapReduce, or distributed computing is popular for better performance.

Data Model—Column-based databases stores data by compressing it. Data is partitioned and distributed.

Scalability—Compression and distribution delivers scalability better than other NoSqls.

Operations—Write operations are faster to load big size of data, loading multimillion rows in column family store takes few seconds. Distributed computing makes data analysis quicker and faster too.

Graph Database. Graph NoSqls stores data and its relationships. Data stored as nodes and edges [9]. Node stores data about the entity and edges are relation between nodes. This pair of node and edge defines object mode similar to entity relation model. Nodes can have their attributes. In relational databases, referential integrity is maintained as foreign key and primary key relationship likewise graph databases stores relations in edges. Relational databases are fixed schema data stores and it is difficult to add new referential data in the fixed schema data stores but in graph stores random addition of relations is an easy operation.

We can add properties to the edges to inherit intelligence to databases relations. New relations to the graph database are easy operation but modification in edges is difficult. It means a change in each node. It is critical to select right relationship and properties first time as most of the query results dependent on edge or relations.

Example of popular graph databases are—Neo4J, Infinite Graph, OrientDB, FlockDB.

For example. Directions, routes, maps distance related uses case of more popular applications for graph databases. Anomaly detection, fraud detection, and other use case of generally applied for graph databases.

4 Choosing Right NoSQL

4.1 *The Data Storage Pattern*

Use case data needs to store in the data model supported by the selected NoSQL. A balance between the NoSQL data structure and the application is critical factor in deciding right NoSQL for the set of applicable use cases [5].

4.2 *Scalability Needs*

What is data sizing size need to process? And what are performance parameters needed to satisfy? These are predominant questions to decide scaling needs for a NoSQL database. Scaling needs are another important factor to decide right NoSql for the application.

4.3 *CAP Theorem*

Concept of CAP theorem is based on three different measurements C-consistency, A-accessibility, and P-partition tolerance in NoSQL database systems [10]. CAP theorem also explains that any single NoSQL cannot have all these capabilities of CA and P at given instance.

4.4 *Narrow the NoSQL Choices Through CAP Theorem*

The CAP theorem explains trade-offs between ACID and BASE and concludes that in a distributed data store, only two of the CA and P can be guarantee for a distributed database. Consistency, availability, and partition tolerance, all three ability is not possible to achieve [10].

- Consistency: Even though data is stored at different node and data can be read from multiple nodes, bur response to a read query needs to be exactly same based upon latest data write. The node which is responding the query should not change the query output; in other words, query output should be consistent on every node in the cluster.
- Availability: In case of node failure, other node should response to query or perform write operation and in case of one or few nodes, failure database should be available and functioning.

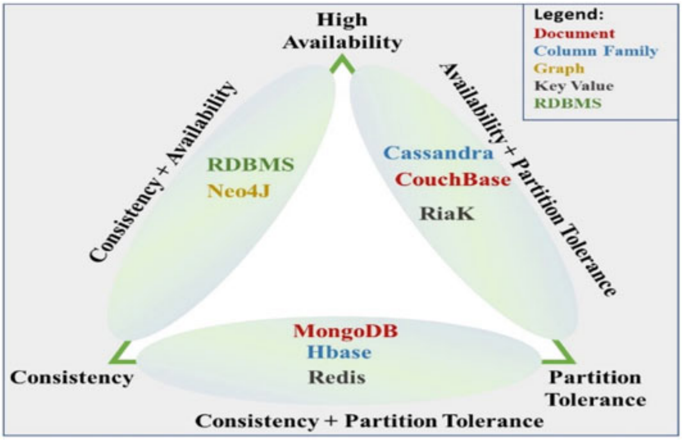


Fig. 1 NoSQL positioning based On CAP theorem

- Partition tolerance: The data distributions and storage partitions need to design such a way that in case of hardware failure or node failure, data can be recovered, and queries are responded in certain time.

According to the CAP theorem, only two of the three CA, CP, or AP attributes can be available of the data store. Selection of NoSQL based on the applicability of these attributes is one of the least risky way of NoSQL database selection (Fig. 1).

5 Determine NoSQL Database Type

Most of the database selection is done based upon the target application and its use cases for obvious reasons [11]. Here are listing of some key use cases for each NoSQL database type. This is to set up guidelines while classifying application requirements at early stage of application data store feature definition.

5.1 Select Criteria of Key-Value Database

- No complex data structure
- Large number of simultaneous query/insert with minimum updates
- High scalability and quicker performance
- Simple queries no joins.

5.2 Select Criteria of Document Stores If

- Unstructured or semi-structured data
- Complex query and schemeless data
- JSON or XML data store or query interface
- Multilevel index support
- Quicker performance and consistency
- No joins or dynamic relations.

5.3 Choose Column-Oriented Database If

- Big data volume
- Faster write performance than read performance
- Row key-based queries
- No ad hoc query patterns, complex indices, or high level of aggregations.

Based on different NoSQL database comparisons, it is considered that for an enterprise, there will be multiple types of NoSQL databases that will need based on the application and use case [12]. Some organizations will need a combination of graph database and document databases, whereas some will need key-value pair and document databases.

6 Conclusion—A Multi-model Technology Consolidation

The above-mentioned NoSQL database types and their advantages lead to the multi-model database. A multi-model database which is another popular option combines the various NoSQL database types. It means more versatility for you—the end-user—in the way you store your data.

A significant portion of large enterprise strategies is dependent on analytics or prediction which is derived. Customer experience, high agility, and a large volume of data are making the pressing need for NoSQL databases, a critical component of the analytics ecosystem [13].

Because each type of NoSQL database serves significantly different uses cases, an enterprise needs at least one of each type of NoSQL database to obtain the best coverage and technology utilization. While planning technology considerations, it is important not to consolidate or sunset different types of NoSQL. Even though there are many similar functionalities offered by these NoSQL databases, the performance of additional services or implementation ease of the services creates a lot of barriers in the long run; for example, graph databases cannot replace document databases for online scalable web applications.

Technology consolidation is highly recommended for the same type of NoSQL databases and not recommended between different types of NoSQLs.

References

1. Kumar KBS, Srividya, Mohanavalli S (2017) A performance comparison of document-oriented NoSQL databases. https://doi.org/10.1109/icccsp.2017.7944071
2. Schulz WL, Felker Thomas DK, Durant RichardTorres JS (2016) Evaluation of Relational & NoSQL database architectures to manage genomic annotations. https://doi.org/10.1016/j.jbi.2016.10.015
3. Gurevich Y (2015) Comparative survey of NoSQL/NewSQL DB System
4. Aqel MJ, Al-Sakran A, Hunaity MA (2019) Comparative study of NoSQL databases. Biosc Biotech Res Comm. https://bit.ly/2XofzId
5. Rafique A, Joosen W, Lagaisse B, Van Landuyt D (2018) A study of the trade-off between performance and migration cost. https://doi.org/10.1109/TCC.2015.2511756
6. Pereira A, Ourique de Morais W, Pignaton de Freitas DE (2017) NoSQL real-time database performance comparison. Int J Parallel Emergent Distrib Syst. https://doi.org/10.1080/17445760.2017.1307367
7. Van Landuyt R, Rafique V (2017) AD. et al. Object—NoSQL database mappers: a benchmark study on the performance overhead. https://doi.org/10.1186/s13174-016-0052-x
8. Naheman W, Wei J (2013) Review Of NoSQL databases & performance testing on HBase. https://doi.org/10.1109/mec.2013.6885425
9. Plechawska-Wojcik M, Damian R (2016) Comparison of relational, document & graph databases in the context of the web application development. https://doi.org/10.1007/978-3-319-285610_1
10. Gilbert S, Lynch NA (2000) Perspectives on the CAP theorem. https://groups.csail.mit.edu/tds/papers/Gilbert/Brewer2.pdf
11. Tappert C, Perez G, Mackin H (2016) Adopting NoSQL Databases using a quality attribute framework and risks analysis, pp 97–104. https://doi.org/10.5220/0006227600970104. ISBN: 978-989-758-200-4
12. Tang F-Y, Fan Y (2016) Performance Comparison between five NoSQL databases. In: 7th international conference on cloud computing and big data (CCBD). 10.1.1109/CCBD.2016.030, Corpus ID:22633936
13. Mackin H, Perez G, Tappert C (2016) Adopting NoSQL databases using a quality attribute framework and risks analysis. In: Proceedings of the fifth international conference on telecommunications and remote sensing—ICTRS. ISBN 978-989-758-200-4, pp 97–104. https://doi.org/10.5220/0006227600970104

A Review on Proteomic Function Prediction in Pathogenic Bacterial Organism Using Machine Learning

Anushri Vijay, Neha Tiwari, and Amita Sharma

Abstract In the realm of health research and the medical business, machine learning plays a vital role. In today's world, protein research is critical in the development of medicinal drugs. Proteins are responsible for the structure, function, and regulation of our biological tissues, organ functionality as well as the majority of cell work. A pathogen is an organism that can infect its host and causes disease, and virulence refers to the severity of the symptoms. Some infections are only able to live in specific hosts. Other diseases can infect a broad array of species. It is easy to identify the characteristics and behavior of known bacterial proteins but the prediction of unknown proteins is a cumbersome task. The paper discusses the objectivity of machine learning in predicting the unknown proteins along with their functions, specifically in harmful bacterial species.

Keywords Machine learning · Pathogen · Bacteria · Proteomic · Bioinformatics · Unknown proteins

1 Introduction

In health research and the medical business domain, proteomics has a wide spectrum of research. In today's world, protein research is crucial in the development of medicinal drugs. Proteins are an indispensable part of every living organism. The study of unknown bacterial proteins is far more complex as compared to other microorganisms such as yeast, algae, and fungus, as bacteria have a tremendous capacity to mutate [1]. Hypothetical (unknown) protein function prediction is a time-consuming as well as a costly affair when it comes to wet-lab testing procedures. Using machine learning in predicting these unknown protein functions explicitly concerning harmful bacterial species opens up a promising research area.

A. Vijay (✉) · N. Tiwari · A. Sharma
IIS (Deemed To Be University), Jaipur, India
e-mail: anushrivijay31890@iisuniv.ac.in

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6_80

1.1 Background

The study of all proteins made up of long chains of 20 amino acid residues is known as proteomic research. The proteome is a collection of proteins found in living organisms. Proteomic research currently provides a substantial amount of genetic data to all genomics studies. When proteomics and genomic research are combined, biomedical research and the development of next-generation diagnostic and therapeutic tools can be revolutionized [2]. The discovery of therapeutic drugs requires the study of pathogenic species which are microorganisms that can inflict bacterial infections. Bacterial organisms are huge and complicated, and they evolve quickly; therefore, performing a wet-lab experiment for each new bacterium protein function prediction [3] is a tough and time-consuming operation. As a result, a computing machine should be constructed to produce the result more quickly and at a lower cost. Machine learning technology is the computational technique that by examining and extracting inferences from data using algorithms and statistical models, they may learn and adapt without following explicit instructions.

2 Pathogenic Bacterial Species

A pathogen is a disease-causing organism. A significant number of microorganisms live in human bodies. When our immune system is weakened while bacteria penetrate a typically sterile area of our bodies, we have a problem. They only need a host to develop and live. The infection avoids immune reactions and replicates using the body’s energies while inside the host’s body before leaving and spreading to a new target. Understanding disease microorganisms is vital because bacteria are more complicated and larger than viruses, move through the air, are extremely adaptable, and can quickly change to resist treatments.

Bacteria evolve at a rapid rate on their own, resulting in a proliferation of bacterial entities. As a result, determining the function of newly generated bacteria proteins is difficult. Proteins are used by bacteria for a range of functions, including structure, enzymes, and transportation. Antibiotics that restrict protein synthesis are used to treat bacterial infections. Bacteria, in general, have both known and unknown proteins (hypothetical proteins (HPs)) [4]. In a variety of animals, HPs can play a critical role in pathogen survival and the advancement of infectious diseases. As a consequence, annotating all of these novel bacterium species in wet labs is a time-consuming and challenging operation.

Multiple infections are caused by pathogenic germs. A substantial number of HPs are found in all of these pathogenic microorganisms. Urine tract infection (UTI), for example, is a frequent infectious condition caused by harmful bacteria. Table 1 lists a few common UTI bacteria along with their HPs status. Bacteria are also responsible for food and waterborne infections. A few common pathogens are included in Table 2.

Table 1 Pathogenic bacteria species specifying UTI source, cause of infection, their known and unknown protein, and their strain property [5]

Pathogenic bacteria	Source	Infection caused	Total proteins	Unknown proteins	Gram Stain
Citrobacter freundii	Water, soil, food, and the intestinal tracts of animals and humans	UTIs, wound, respiratory, meningitis, and sepsis	211,502	48,429 (22.89%)	Gram-negative
Klebsiella Oxytoca	Directly exposed to pathogens, bacteria are disseminated through person-to-person contact, and bacteria are acquired from a contaminated environment KO is not transmitted through the air	Pneumonia, septicemia, UTI, and soft tissue infection	100,756	12,735 (12.6%)	Gram-positive
Serratia marcescens	Water, soil, animals, insects, and plants	UTIs, respiratory tract infections, conjunctivitis, tear duct infections, keratitis, pneumonia, and meningitis in rare cases	305,440	36,806 (12.05%)	Gram-negative
Morganella morganii	Water, soil, and the intestinal tracts of mammals	Sepsis, abscess, purple urine bag syndrome, chorioamnionitis, and cellulitis (during pregnancy)	124,169	19,642 (15.81%)	Gram-negative

When the stain reacts with the bacteria in a sample, they will either stay purple or turn pink or red
*Gram-positive stain—The color purple is retained by gram-positive bacteria
*Gram-negative stain—When gram-negative bacteria are exposed to a gram-negative stain, their pink color turns white

Table 2 Pathogenic bacteria species specifying the foodborne and waterborne source, cause of infection, their known and unknown protein, and their stain property [5]

Pathogenic bacteria	Source	Infection caused	Total proteins	Unknown proteins	Gram Stain
Clostridium botulinum	(a) Home-canned foods (b) Spicy peppers (chiles), foil-wrapped baked potato (c) Oil infused with garlic	Botulism disease is caused by the Clostridium botulinum bacteria's toxins (a) Botulism caused by food (b) Botulism caused by wounds, and (c) Botulism caused by infants	161,856	32,677 (20.1%)	Gram-positive
Providencia alcalifaciens	Soil, water, and sewage	Ingestion of contaminated foods	33,438	5575 (16.67%)	Gram-negative
Cronobacter	Dry foods, like powdered infant formula, powdered milk, herbal teas, and starches, sewer water	consumption of reconstituted powdered infant formula	264,502	30,778 (11.63%)	Gram-negative
Photobacterium damselae	Marine animals and also humans	Necrotizing fasciitis with fatal outcome	54,769	8450 (15.42%)	Gram-negative
Aeromonas hydrophila	Gastroenteritis (ingestion of contaminated water or food) and wound infections (exposure to contaminated water)	A broad-spectrum of infections (septicemia, meningitis, endocarditis)	143,989	18,319 (12.72%)	Gram-negative
Salmonella enterica	Food and water, by direct animal contact, and rarely from person to person	Ingestion of contaminated food, eating raw, or undercooked meat, poultry, eggs, or egg products	1,022,367	110,804 (10.83%)	Gram-negative
Vibrio cholera	1. Surface or well water 2. Seafood 3. Raw fruits and vegetables 4. Grains	Severe diarrhea and dehydration	871,724	39,720 (4.55%)	Gram-negative

As indicated in Tables 1 and 2, hypothetical UTI pathogenic bacteria proteins account for 15.85% of the 741,867 known proteins, whereas hypothetical food and waterborne pathogenic bacteria proteins account for 9.64% of the 2,552,645 known proteins.

In biochemistry, a hypothetical protein is one whose existence has been anticipated but for which no experimental proof of expression in vivo exists. The sequencing of multiple genomes has resulted in a large number of predicted open reading frames with unknown functions. Several studies have been conducted in the past to look at the functions of HPs in various illnesses. The identification and characterization of hypothetical proteins can help in therapeutic target selection. HPs may serve as possible new drug targets because of their limited homology and relatedness to other known proteins [3].

To bridge the gap between the "knowns" and the "unknowns," efforts to get a fundamental idea of the roles and possible functions of HPs are vital. This is notably critical for fitting and completing the genetic information jigsaw of every living thing, as well as gaining a "full" understanding of these organisms as biological systems.

HP protein function prediction is a difficult endeavor that demands extensive testing. Machine learning algorithms have evolved in recent years to determine protein functions utilizing existing experimental result datasets. These methods are both cost-effective and lower the number of lab tests required. The literature on ML-based protein function prediction in pathogenic species is described in the next section.

3 Protein Function Prediction in Pathogenic Species

Understanding the function of proteins in disease pathobiology, metagenome activities and therapeutic target discovery require a significant amount of bioinformatics work. Homology-based techniques, methods based on sequence motifs, methods based on structure, and methods based on the context of the genome are some of the traditional molecular biology-based methodologies used to predict or determine the functions of a certain protein. Genome sequencing and sophisticated lab experiments are commonly used in these approaches, which are time demanding, costly, and take a considerable amount of resources. To optimize the cost and time, there is a need to deploy a computational technique that controls these parameters. Machine learning (ML) is one such technology that can be used to predict protein function based on known protein characteristics. Similarly, an unknown bacterial species' protein function might be discovered from known bacterial species using a protein–protein interaction tool and machine learning (dry lab experiment) in a matter of minutes. All it needs is a well-annotated dataset. A brief description of machine learning is presented in the next section.

4 Machine Learning

Learning is a crucial component of machine learning. Learning is the process of obtaining new knowledge, developing new abilities, changing one's behavior, and gaining previous experience.

Machine learning consists of three types: (a) supervised learning (b) unsupervised learning (c) reinforcement learning (see Fig. 1). Supervised learning is the practice of using labeled datasets to train computers to reliably identify data or predict outcomes. Unsupervised learning is the process of learning to find patterns in data sets that contain no classified or labeled data items [6]. Machine learning models are taught to make a series of judgments via reinforcement learning. The exponential growth of biomedical data has inspired the application of several machine learning algorithms to address new challenges in biology and clinical research in recent years.

To comprehend the new challenges posed by sickness produced by hazardous bacterial organisms, we must research the characteristics and properties of proteins. Machine learning has been used to develop protein function, prediction models in a few studies.

To better understand protein function prediction using machine learning, a study of the literature was conducted (as shown in Table 3).

This literature review concludes that ML is quite suitable for finding protein function. Hypothetical (unknown) protein can be easily studied using ML, as it can reduce search space for wet-lab experiments. As a result, we can deduce that supervised machine learning is the most widely utilized machine learning method.

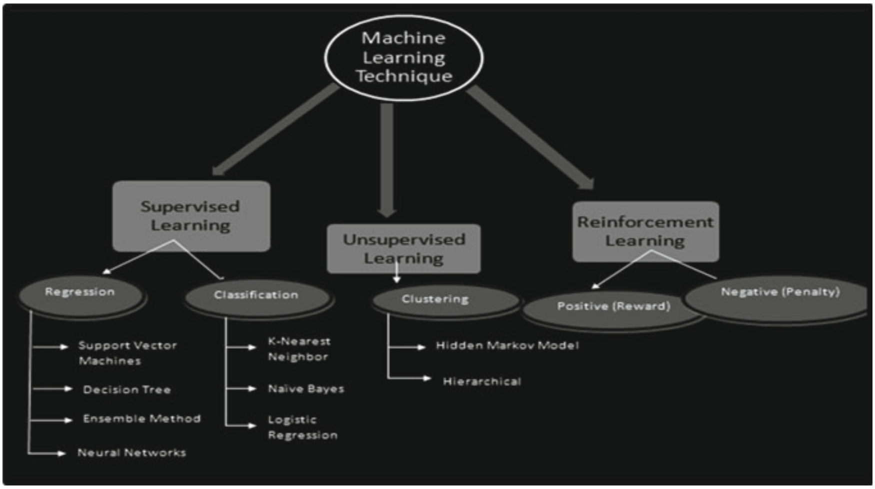


Fig. 1 Types of machine learning

Table 3 Review of the literature on the use of machine learning to predict pathogenic species protein functions

Title	Year and Author	Objectives	Technique used	Conclusion
Predicting host dependency factors of pathogens in Drosophila melanogaster using machine learning	[7]	The study used machine learning to predict host dependency factors (HDF)	Gold standard machine learning	The objectiveness of host-dependent elements in drug design can be exploited. They provided a list of 208 HDF novels for future experimentation
A review: antimicrobial resistance data mining models and prediction methods study for pathogenic bacteria	[8]	This study reviewed antimicrobial resistance, ML techniques, evaluation methods, and associated risk assessment approaches	NA	Challenges listed by authors are:- (1) Lack of database homogeneity (2) Lack of surveillance, therapeutic usage, and resistance in livestock (3) There are currently no fully functional models for predicting which resistance genes would spread locally in the healthcare system and globally across countries
A deep learning ensemble for function prediction of hypothetical proteins from pathogenic bacterial species	[9]	The goal of this research is to study bacterial species using machine learning	Deep neural network	They used a combination of features based on sequence, physicochemical property, subsequence, and annotation features of protein to design a model. The deep learning ensemble model based on the deep neural network technique is successful, with an accuracy of 0.7912

(continued)

Table 3 (continued)

Title	Year and Author	Objectives	Technique used	Conclusion
A model to predict the function of hypothetical proteins through a nine-point classification scoring schema	[3]	The goal of this research is to come up with novel ways to interpret the a) sequence b) structure–function relationship, especially in the context of HP functional modeling, but no attempt has been made to use the features as HP classifiers	NA	This study presented a nine-point methodology for classifying hypothetical proteins as known or unknown
Predicting protein function via multi-label supervised topic model on gene ontology	[10]	They designed a model in which a protein is considered as a sentence and function is a label in the investigation Used yeast and human protein data set	multi-label supervised topic model	The multi-label predictive model applies to an HP and their functions can be defined

5 Conclusion and Future Scope

Finally, we came to a conclusion in Tables 1 and 2 conducted a case study to analyze the unknown proteins identified in bacterial species. Hypothetical UTI pathogenic bacteria proteins, for example, account for 15.85% of the 741,867 known proteins, whereas food and waterborne pathogenic bacterial proteins account for 9.64% of the 2,552,645 known proteins. The high cost of instrument maintenance, which includes replacement parts, reagents, consumables, and periodic inspections, could stifle protein analysis expansion. As a result, computational techniques can be used with little effort and time. We conducted a literature review and looked at a variety of machine learning techniques, the most prevalent of which being supervised learning, in this study. The design of machine learning algorithms, as well as the prediction of new data mining analytical functions, is all hot subjects in bioinformatics right now.

Simultaneously, the multidisciplinary approach has aided the advancement of machine learning. As a result, protein function prediction has numerous applications, including food and non-food packaging, healthcare, drug discovery, and disease etiology. Research into unknown protein function prediction will greatly improve the development of new drugs. Machine learning techniques are extremely useful for forecasting and discovering trends in massive datasets. Data mining architecture, machine learning algorithm development, and new data mining analysis function prediction are all hot topics in bioinformatics right now. Exploring unknown protein function prediction will greatly improve the development of novel drugs.

References

1. Wen B, Zhang B (2020) Computational proteomics: focus on deep learning. Proteomics 20(21–22):2000258. https://doi.org/10.1002/pmic.202000258
2. Dupree EJ, Jayathirtha M, Yorkey H, Mihasan M, Petre BA, Darie CC (2020) A critical review of bottom-up proteomics: the good, the bad, and the future of this field. Proteomes 8(3):14. https://doi.org/10.3390/proteomes8030014
3. Ijaq J, Malik G, Kumar A, Das PS, Meena N, Bethi N, Sundararajan VS, Suravajhala P (2019) A model to predict the function of hypothetical proteins through a nine-point classification scoring schema. BMC Bioinformatics 20(1). https://doi.org/10.1186/s12859-018-2554-y
4. Yang Z, Zeng X, Tsui SKW (2019b) Investigating function roles of hypothetical proteins encoded by the Mycobacterium tuberculosis H37Rv genome. BMC Genomics 20(1). https://doi.org/10.1186/s12864-019-5746-6
5. Access NCBI through the World Wide Web (WWW) (1995) Molecular Biotechnology 3(1):75. https://doi.org/10.1007/bf02821338
6. Yang H, An Z, Zhou H, Hou Y (2018) Application of machine learning methods in bioinformatics. Application of Machine Learning Methods in Bioinformatics. Published. https://doi.org/10.1063/1.5039089
7. Aromolaran O, Beder T, Adedeji E, Ajamma Y, Oyelade J, Adebiyi E, Koenig R (2021) Predicting host dependency factors of pathogens in Drosophila melanogaster using machine learning. Comput Struct Biotechnol J 19:4581–4592. https://doi.org/10.1016/j.csbj.2021.08.010

8. Li X, Zhang Z, Liang B, Ye F, Gong W (2021) A review: antimicrobial resistance data mining models and prediction methods study for pathogenic bacteria. J Antibiot 74(12):838–849. https://doi.org/10.1038/s41429-021-00471-w
9. Mishra S, Rastogi YP, Jabin S, Kaur P, Amir M, Khatun S (2019) A deep learning ensemble for function prediction of hypothetical proteins from pathogenic bacterial species. Comput Biol Chem 83:107147. https://doi.org/10.1016/j.compbiolchem.2019.107147
10. Liu L, Tang L, He L, Yao S, Zhou W (2017) Predicting protein function via multi-label supervised topic model on gene ontology. Biotechnol Biotechnol Equip 31(3):630–638. https://doi.org/10.1080/13102818.2017.1307697

Author Index

X.-S. Yang et al. (eds.), *Proceedings of Seventh International Congress on Information and Communication Technology*, Lecture Notes in Networks and Systems 448,
https://doi.org/10.1007/978-981-19-1610-6