

Lecture Notes in Networks and Systems 459

Suresh Chandra Satapathy ·
Jerry Chun-Wei Lin · Lai Khin Wee ·
Vikrant Bhateja · T. M. Rajesh *Editors*

Computer Communication, Networking and IoT

Proceedings of 5th ICICC 2021, Volume 2

 Springer

Lecture Notes in Networks and Systems

Volume 459

Series Editor

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences,
Warsaw, Poland

Advisory Editors

Fernando Gomide, Department of Computer Engineering and Automation—DCA,
School of Electrical and Computer Engineering—FEEC, University of
Campinas—UNICAMP, São Paulo, Brazil

Okay Kaynak, Department of Electrical and Electronic Engineering,
Bogazici University, Istanbul, Turkey

Derong Liu, Department of Electrical and Computer Engineering, University of
Illinois at Chicago, Chicago, USA

Institute of Automation, Chinese Academy of Sciences, Beijing, China

Witold Pedrycz, Department of Electrical and Computer Engineering, University of
Alberta, Alberta, Canada

Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

Marios M. Polycarpou, Department of Electrical and Computer Engineering,
KIOS Research Center for Intelligent Systems and Networks, University of Cyprus,
Nicosia, Cyprus

Imre J. Rudas, Óbuda University, Budapest, Hungary

Jun Wang, Department of Computer Science, City University of Hong Kong,
Kowloon, Hong Kong

The series “Lecture Notes in Networks and Systems” publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

Suresh Chandra Satapathy · Jerry Chun-Wei Lin ·
Lai Khin Wee · Vikrant Bhateja · T. M. Rajesh
Editors

Computer Communication, Networking and IoT

Proceedings of 5th ICICC 2021, Volume 2


 Springer

Editors

Suresh Chandra Satapathy
School of Computer Engineering
Kalinga Institute of Industrial Technology
Bhubaneswar, India

Lai Khin Wee
University of Malaya
Kuala Lumpur, Malaysia

T. M. Rajesh
Department of Computer Science
and Engineering
Dayananda Sagar University
Bengaluru, India

Jerry Chun-Wei Lin 
Western Norway University of Applied
Sciences
Bergen, Norway

Vikrant Bhateja
Department of Electronics
and Communication Engineering
Shri Ramswaroop Memorial College
of Engineering and Management
(SRMCEM)
Lucknow, Uttar Pradesh, India

Dr. A.P.J. Abdul Kalam Technical
University
Uttar Pradesh, India

ISSN 2367-3370

ISSN 2367-3389 (electronic)

Lecture Notes in Networks and Systems

ISBN 978-981-19-1975-6

ISBN 978-981-19-1976-3 (eBook)

<https://doi.org/10.1007/978-981-19-1976-3>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Conference Organization Committee

Chief Patrons

Dr. D. Hemachandra Sagar, Chancellor, DSU, Chairman DSI

Dr. D. Premachandra Sagar, Pro-Chancellor, DSU, Chairman DSI

Patrons

Shri. Galiswamy, Secretary, DSI

Dr. K. N. B. Murthy, Vice Chancellor, DSU

Shri. R. Janardhan, Pro-Vice Chancellor, DSU

Dr. Puttamadappa C., Registrar, DSU

Honorary Chairs

H. P. Khincha, Evangelist, DSU

K. Jairaj, Advisor, DSU

General Chair

Dr. S. C. Satapathy, KIIT, Bhubaneshwar, Odisha, India

Dr. Yudong Zang, University of Leicester, UK

Publication Chair

Dr. Vikrant Bhateja, SRMCEM, Lucknow, UP, India
Dr. Jerry Chun-Wei Lin, Western Norway University of Applied Sciences, Bergen, Norway

Organizing Chairs

Dr. M. K. Banga, Dean Research, DSU
Dr. A Srinivas, Dean SoE, DSU

Technical Program Chairs

Dr. Ranjita Das, National Institute of Technology (NIT), Mizoram, India
Dr. Lai Khin Wee, University of Malaya, Kuala Lumpur, Malaysia

Program Chairs

Dr. T. M. Rajesh, Department of CSE, DSU
Dr. Shaila S. G., Department of CSE, DSU
Dr. Girisha G. S., Department of CSE, DSU

Advisory Committee

Dr. Aime' Lay-Ekuakille, University of Salento, Lecce, Italy
Dr. Amira Ashour, Tanta University, Egypt
Dr. Aynur Unal, Stanford University, USA
Dr. Bansidhar Majhi, IIIT Kancheepuram, Tamil Nadu, India
Dr. Dilip Kumar Sharma, Vice Chairman, IEEE UP Section
Dr. Ganpati Panda, IIT Bhubaneswar, Odisha, India
Dr. Jagdish Chand Bansal, South Asian University, New Delhi, India
Dr. João Manuel R. S. Tavares, Universidade do Porto (FEUP), Porto, Portugal
Dr. Jyotsana Kumar Mandal, University of Kalyani, West Bengal, India
Dr. K. C. Santosh, University of South Dakota, USA
Dr. Le Hoang Son, Vietnam National University, Hanoi, Vietnam
Dr. Naeem Hanoon, Multimedia University, Cyberjaya, Malaysia

Dr. Nilanjan Dey, TIET, Kolkatta, India
Dr. Noor Zaman, Universiti Teknologi, PETRONAS, Malaysia
Dr. Roman Senkerik, Tomas Bata University, Zlin, Czech Republic
Dr. Swagatam Das, Indian Statistical Institute, Kolkatta, India
Dr. Siba K. Udgata, University of Hyderabad, Telangana, India
Dr. Shri Nivas Singh, MMMUT, Gorakhpur, UP, India
Dr. Steven L. Fernandez, The University of Alabama at Birmingham, USA
Dr. Tai Kang, Nanyang Technological University, Singapore
Dr. Valentina Balas, Aurel Vlaicu University of Arad, Romania

Technical Program Committee

Abdul Rajak A. R., Department of Electronics and Communication Engineering, Birla Institute of Dr. Nitika Vats Doohan, Indore, India
Ahmad Al-Khasawneh, The Hashemite University, Jordan
Alexander Christea, University of Warwick, London, UK
Amioy Kumar, Biometrics Research Lab, Department of Electrical Engineering, IIT Delhi, India
Anand Paul, The School of Computer Science and Engineering, South Korea
Apurva A. Desai, Veer Narmad South Gujarat University, Surat, India
Avdesh Sharma, Jodhpur, India
A. K. Chaturvedi, Department of Electrical Engineering, IIT Kanpur, India
Bharat Singh Deora, JRN RV University, India
Bhavesh Joshi, Advent College, Udaipur, India
Brent Waters, University of Texas, Austin, Texas, United States
Chhaya Dalela, Associate Professor, JSSATE, Noida, Uttar Pradesh
Dan Boneh, Computer Science Department, Stanford University, California, USA
Feng Jiang, Harbin Institute of Technology, China
Gengshen Zhong, Jinan, Shandong, China
Harshal Arolkar, Immd. Past Chairman, CSI Ahmedabad Chapter, India
H. R. Vishwakarma, Professor, VIT, Vellore, India
Jayanti Dansana, KIIT University, Bhubaneswar, Odisha
Jean Michel Briel, Departement Informatique IUT de Blagnac, Blagnac, France
Jeril Kuriakose, Manipal University, Jaipur, India
Jitender Kumar Chhabr, NIT, Kurukshetra, Haryana, India
Kalpana Jain, CTAE, Udaipur, India
Komal Bhatia, YMCA University, Faridabad, Haryana, India
Krishnamachar Prasad, Department of Electrical and Electronic Engineering, Auckland, New Zealand
K. C. Roy, Principal, Kautaliya, Jaipur, India
Lorne Olfman, Claremont, California, USA
Martin Everett, University of Manchester, England
Meenakshi Tripathi, MNIT, Jaipur, India

Mukesh Shrimali, Pacific University, Udaipur, India
Murali Bhaskaran, Dhirajlal Gandhi College of Technology, Salem, Tamil Nadu, India
Nilay Mathur, Director, NIIT Udaipur, India
Ngai-Man Cheung, Assistant Professor, University of Technology and Design, Singapore
Philip Yang, PricewaterhouseCoopers, Beijing, China
Pradeep Chouksey, Principal, TIT College, Bhopal, MP, India
Prasun Sinha, Ohio State University Columbus, Columbus, OH, USA
Rajendra Kumar Bharti, Assistant Professor, Kumaon Engineering College, Dwarahat, Uttarakhand, India
R. K. Bayal, Rajasthan Technical University, Kota, Rajasthan, India
Sami Mnasri, IRIT Laboratory Toulouse, France
Savita Gandhi, Professor, Gujarat University, Ahmedabad, India
Soura Dasgupta, Department of TCE, SRM University, Chennai, India
Sushil Kumar, School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India
S. R. Biradar, Department of Information Science and Engineering, SDM College of Engineering and Technology, Dharwad, Karnataka
Ting-Peng Liang, National Chengchi University Taipei, Taiwan
Xiaoyi Yu, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing, China
Yun-Bae Kim, SungKyunKwan University, South Korea

Preface

This book is a collection of high-quality peer-reviewed research papers presented at the “5th International Conference on Intelligent Computing and Communication (ICICC 2021)” held at School of Engineering, Dayananda Sagar University, Bengaluru, India, during November 26 to 27, 2021.

After the success of the past four editions of ICICC conferences held in 2016 at University of Kalyani, West Bengal, India, in 2017 at MAEER’s MIT College of Engineering, Pune, India, and in 2019 and 2020 at SoE, Dayananda Sagar University, Bengaluru, India, the 5th International Conference on Intelligent Computing and Communication is organized by Dayananda Sagar University, School of Engineering, Bengaluru, India. All the papers of past ICICC editions are published by Springer Nature as publication partner. Presently, ICICC 2021 provided a platform for academicians, researchers, scientists, professionals, and students to share their knowledge and expertise in the diverse domain of intelligent computing and communication.

ICICC 2021 had received a number of submissions from the field of ICT, intelligent computing, and its prospective applications in different spheres of engineering. The papers received have undergone a rigorous peer-review process with the help of the technical program committee members of the conference from the various parts of the country as well as abroad. The review process has been crucial with minimum of two reviews, each along with due checks on similarity and content overlap. This conference has featured five exclusive theme-based special sessions as enlisted below along with the main track:

Special Session 1: “Empirical Software Engineering (ESE)”

Special Session 2: “Artificial Intelligence and Space Technology for Climate Smart Agriculture and Disaster Risk Reduction in Hyperlocal Scenario (AIST-CSADRR)”

Special Session 3: “AI and Machine Learning Applications for Cyber Security”

Special Session 4: “Computer Vision and Machine Learning (CVML)”

Special Session 5: “Emerging Trends in Cognitive Computing and Deep Learning (ETCDL)”

The conference featured many distinguished keynote addresses by eminent speakers like: Dr. Kavi Mahesh, Director, Indian Institute of Information Technology, Dharwad, who addressed the gathering on the topic computing and intelligence. Mr. Vishwanath Sastry, Associate Vice President, Harman International, Stanford, USA, delivered a lecture on IoT and analytics. Dr. Kartik Gopalan, Professor in Computer Science at the Binghamton University, USA, Associate Editor of IEEE Transactions on Cloud Computing, delivered a lecture on nesting to bare-metal: strange adventures in the virtual world. Dr. Govindarasu Manimaran, Professor of Electrical and Computer Engineering at the Iowa State University, USA, delivered a lecture on cybersecurity for critical infrastructures in the information age.

These keynote lectures/talks embraced a huge toll of audience of students, faculties, budding researchers as well as delegates. The editors thank the General Chair, TPC Chair, and the Organizing Chair of the conference for providing valuable guidelines and inspirations to overcome various difficulties in the process of organizing this conference. The editors also thank School of Engineering, Dayananda Sagar University, Bengaluru, for their whole-hearted support in organizing this edition of ICICC conference series.

The editorial board take this opportunity to thank authors of all the submitted papers for their hard work, adherence to the deadlines, and patience during the review process. The quality of a refereed volume depends mainly on the expertise and dedication of the reviewers. We are indebted to the TPC members who not only produced excellent reviews but also did these in short time frames.

Lucknow, India
Kuala Lumpur, Malaysia
Bergen, Norway
Bhubaneswar, India
Bengaluru, India

Dr. Vikrant Bhateja
Dr. Lai Khin Wee
Dr. Jerry Chun-Wei Lin
Dr. Suresh Chandra Satapathy
Dr. T. M. Rajesh

Contents

Cloud-Based E-learning: Scaffolding the Environment for Adaptive E-learning Ecosystem Based on Cloud Computing Infrastructure	1
Ashraf Alam	
Web Crawling-Based Search Engine for Programming Languages	11
Prachi Medline Ekka and Rupali Kute	
Smart Helmet for Coal Mine Monitoring	23
Riya Yadav, Manish Pandey, and Santosh Kumar Sahu	
K-Weighted Cluster Head Selection in Wireless Sensor Networks	33
T. Siron Anita Susan, B. Nithya, Harshit Agrawal, and Duggirala Vijitendra	
Implementation and Performance Analysis of PEGASIS and MIEEPB Protocols in Wireless Sensor Networks	45
Trupti Shripad Tagare and Rajashree Narendra	
A Queue Management System for Cloud Data Processing	55
Arif Ahmad Shehloo and Muheet Ahmed Butt	
Sensor Integration and Information Sharing for Automated Electric Vehicles for Better Estimation of the Surroundings	67
Naarisetti Srinivasa Rao, Reddy Ganesh, K. R. Raghunandan, D. Radhakrishna, C. Praveenkumar, and Bonthu Kotaiah	
Cloud-Computed Solar Tracking System	75
G. Govinda Rajulu, M. Jamuna Rani, D. Deepa, Udit Mamodiya, Radhika G. Deshmukh, and T. Rajasanthosh Kumar	
Patient Identifier Using Biometric Authentication	87
N. Ramya, N. Mahika Kamale, M. Darahasa, P. Mahitha, and T. Anuradha	

Recognition of Hand Gesture-Based Sign Language Using Transfer Learning	95
B. Lakshmi Ramani, T. Sri Lakshmi, N. Sri Durga, Shaik Sana, T. Sravya, and N. Jishitha	
Robustness Indices of 3R and 4R Planar Serial Manipulators with Fixed Actuation Scheme	105
Shaik Himam Saheb and G. Satish Babu	
Deterioration of Daily Life in COVID-19	117
Shubhangi V. Urkude and D. Saravanan	
A Design Model of Copyright Protection System Based on Distributed Ledger Technology	127
K. Varaprasada Rao and Sandeep Kumar Panda	
Secure Electronic Voting (E-voting) System Based on Blockchain on Various Platforms	143
K. Varaprasada Rao and Sandeep Kumar Panda	
Dynamic Authentication Using Visual Cryptography	153
K. D. Devika and Ashutosh Saxena	
Browser Extension for Digital Signature	163
Yerra Maithri and Ashutosh Saxena	
Design and Implementation of Cyber Threat Intelligence Data Mining Model	171
S. Lakshmi Narayanan, S. Shunmugavel, R. Prasanth, M. Satheesh Kumar, K. Srujan Raju, and K. Suthendran	
Gameplay Cognitive Decision Support Using Statistical and Non-statistical Parametric Fusion	187
K. Srujan Raju, Vinayak Jagtap, Parag Kulkarni, and M. Varaprasad Rao	
Securing Communication in IoT Environment Using Lightweight Key Generation-Assisted Homomorphic Authenticated Encryption	195
Ajeet Singh, Vikas Tiwari, Appala Naidu Tentu, and Ashutosh Saxena	
Gas Leakage Detection and Control System	205
Sanjay Kumar, Durgesh Kumar, Deepanshu, and Abhishek	
Advanced Face Mask Detection System	213
Sanjay Kumar, Sandeep Kumar, Nirmalendu Kumar, and Navneet Bhargava	
Meta-Analysis of Nanostructured Sensors for Toxic Gas Sensing	221
Saumya Srivastava, Tripti Sharma, and Manish Deshwal	

High-Impedance Surface Backed Circular Patch Antenna for Wireless Communications 235
 Akash Kumar Gupta, P. Satish Rama Chowdary, and M. Vamshi Krishna

A Critical Analysis on Attacks and Challenges in VANETs 245
 Y. Sarada Devi and M. Roopa

Development of 5G Array Antenna Using 2 × 1 Power Divider for Enhancing Gain in Wireless Applications 257
 Sreevardhan Cheerla, V. Subbareddy, Syed Noor Mohammad, Moghal Ajarvali, and Nichenamtela Neeraj

Novel Technique for Identification of False Coconuts to Avoid Genetic Diseases Using Classifiers 265
 K. Murali, K. Prasuna, and G. Aloy Anuja Mary

Privacy Preserving Datamining Techniques with Data Security in Data Transformation 275
 Bonagiri Jyothi and V. Naga Lakshmi

Rectangular Slotted Elliptically Placed Compact Antenna For Wide Band Applications at K and Ka Bands 287
 A. V. Swathi, Akash Kumar Gupta, M. S. S. S. Srinivas, B. S. S. V. Ramesh Babu, and P. Satish Rama Chowdary

CAN Intrusion Detection Using Long Short-Term Memory (LSTM) 295
 Srinivasa Rao Nandam, Adouthu Vamshi, and Inapanuri Sucharitha

Analysis of Fuel Cell—Battery and Supercapacitor in Driving the Integrated UPQC 303
 Vodapalli Prakash

A Compact Microstrip Antenna with DGS for Bluetooth Applications 311
 M. Chandra Sekhar, M. Suneel Raja, B. Sai Varshini, A. Gunapreetham, K. Neha, and G. Vishal

A Circularly Polarized Single-Feed Patch Antenna for C-Band Satellite Applications 321
 M. Chandra Sekhar, M. Suneel Raja, and Shaik Samreen Sultana

An Integrated Methodology of TsF-KNN-Based Automated Data Classification and Security for Mobile Cloud Computing 329
 P. Rajendra Prasad, V. Rupa, and K. Helini

Cascaded H-Bridge Multilevel Inverter for PV Applications 339
 P. Srujay, Sd. Abeebunnisa, N. Prasad, K. Hanu Vamshi, and M. Srinivas

Dual-Band Circularly Polarized Pentagon-Shaped Fractal Antenna 353
 V. V. Reddy, K. Ashoka Reddy, B. Ramadevi, A. Vijaya, and B. Komuraiah

Device Design and Modeling of Fin Field Effect Transistor for Low Power Applications 361
Umamaheshwar Soma, E. Suresh, B. Balaji, and B. Ramadevi

A Secure Biometric Novel Approach for Authentication Using Multi-Fingerprint Traits 369
Manoj Kumar Vaddepalli and Adepu Rajesh

Static Hand Gesture Recognition for ASL Using MATLAB Platform ... 379
R. Ravi Kumar, Sallauddin Mohmmad, Shabana, D. Kothandaraman, and Dadi Ramesh

Emotion Recognition Based on Streaming Real-Time Video with Deep Learning Approach 393
M. Sheshikala, Sallauddin Mohmmad, D. Kothandaraman, Dadi Ramesh, and Ranganath Kanakam

Efficient Dynamic Framework to Secure MQTT to Detect Distributed DoS Using Meta Empirical Clustering 403
V. Thirupathi and K. Sagar

Optimal Codebook Construction Method Based on Zadoff-Chu Matrix for Code Division Multiple Access Systems 413
R. Nirmaladevi and K. Kishan Rao

Binary Optimal Low-Correlation Region Sequence Set Construction Method 425
R. Nirmaladevi and K. Kishan Rao

Author Index 435

Editors and Contributors

About the Editors

Suresh Chandra Satapathy is a Ph.D. in Computer Science, currently working as Professor and at KIIT (Deemed to be University), Bhubaneswar, Odisha, India. He held the position of the National Chairman Div-V (Educational and Research) of Computer Society of India and is also Senior Member of IEEE. He has been instrumental in organizing more than 20 International Conferences in India as Organizing Chair and edited more than 30 Book Volumes from Springer LNCS, AISC, LNEE, and SIST Series as Corresponding Editor. He is quite active in research in the areas of swarm intelligence, machine learning, and data mining. He has developed a new optimization algorithm known as Social Group Optimization (SGO) published in Springer Journal. He has delivered number of keynote address and tutorials in his areas of expertise in various events in India. He has more than 100 publications in reputed journals and conference proceedings. Dr. Suresh is in Editorial board of *IGI Global*, *Inderscience*, *Growing Science* journals, and also Guest Editor for *Arabian Journal of Science and Engineering* published by Springer.

Jerry Chun-Wei Lin received his Ph.D. from the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan in 2010. He is currently a full professor with the Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, Bergen, Norway. He has published more than 400 research articles in top-tier journals and conferences, 12 edited books, as well as 33 patents (held and filed, 3 US patents). His research interests include data analytics, soft computing, artificial intelligence/machine learning, optimization, IoT, and privacy preserving and security technologies. He is Editor-in-Chief of the *International Journal of Data Science and Pattern Recognition*. He has recognized as the most cited Chinese Researcher respectively in 2018, 2019, and 2020 by Scopus/Elsevier. He is the Fellow of IET (FIET), a senior member for both IEEE and ACM.

Lai Khin Wee received his Ph.D. from Technische Universitat Ilmenau, Germany and Universiti Teknologi Malaysia (UTM) under DAAD Ph.D. Sandwich Programme. He is currently the Head Programme (Master of Engineering) at Faculty of Engineering, University Malaya. He was appointed as Senior Lecturer in Biomedical Engineering Department, University Malaya in early 2013. Prior to that, besides being recognized by students and peers for his excellence as an educator, his contribution in biomedical imaging and point-of-care devices research has made him a regular recipient (more than 30 awards) of numerous international and national awards: multiples Special Awards and Gold Medals, Best of the Best Awards from ITEX, MTE, i-ENVEX, AiNEX, PECIPTA, BioMalaysia Expo, and other innovation and technology events organized by the ministries agency in Malaysia. As for the global influence, Dr. Lai's research prototype has represented Malaysia to participate iCREATe global challenge organized in Singapore, Thailand, and Japan in 2015, 2016, and 2017, respectively. In addition, he had received conference best presentation award from Fukuoka University Japan in 2015, the Best Sustainable Prototype Award in Digital Wonderland Singapore Expo 2019, awarded Honorable Mention Award in 2020 NSIEC by NCKU Taiwan, IEM Young Engineer Award 2021 by Institute of Engineers Malaysia, and IEEE-EMBS Early Career Achievement Award 2021 by IEEE-EMBS Malaysia Chapter. He upholds his academic pursuit by authoring more than 100 peer-reviewed ISI/WoS- and Scopus-listed publications, proceedings, book chapters, laboratory worksheet, and guidelines (h-index 15). His innovations in his areas of expertise awarded him 16 patents and intellectual property rights and several major government and industries funded projects as principal investigator/co-researchers (completed 22 projects, 10 projects on-going) in collaboration with local and international researchers. Dr. Lai currently heads Advanced Analytic Research Group at Medical Imaging Laboratory and supervised 43 postgraduate students (7 Ph.D. and 18 Master completed, 11 Ph.D. and 7 Master on-going).

Vikrant Bhateja is an associate professor in the Department of Electronics and Communication Engineering (ECE), Shri Ramswaroop Memorial Group of Professional Colleges (SRMGPC), Lucknow (UP), and also the dean (Academics) in the same college. He is doctorate in ECE (Bio-Medical Imaging) with a total academic teaching experience of 18 years with around 180 publications in reputed international conferences, journals and online book chapter contributions; out of which 32 papers are published in SCIE indexed high impact factored journals. Among the international conference publications, four papers have received "Best Paper Award." He has been instrumental in chairing/co-chairing around 25 international conferences in India and abroad as Publication/TPC chair and edited 35 book volumes from Springer-Nature as a corresponding/co-editor/author on date. He is Editor-in-Chief of IGI Global—*International Journal of Natural Computing and Research (IJNCR)* an ACM and DBLP indexed journal since 2017. He has guest edited Special Issues in reputed SCIE indexed journals under Springer-Nature and Elsevier.

T. M. Rajesh has completed his Ph.D in January, 2017, from Department of CS&E, Jain University, Bengaluru. He carried out his research on Forensic Crime Detection area in Digital Image Processing and Pattern Recognition domain. Dr. Rajesh has Total of 8+ years of experience in industry, research, and academics domains. He has two years of industrial experience at IGATE Global Solutions Ltd, Bangalore. In IGATE, he worked as Software Engineer for production Support for a client (RTBA and Westpac bank) in Australia. Rajesh is currently guiding 3 Ph.D. research scholars in DIP, PR, CV and ML domains. His publications toward his research work include—7 Indian patents and 2 Australian patents in IoT and computer vision domains, 1 textbook in forensic crime detection area (multi-lingual signature identification and verification in forgery domain), 3 book chapters, 15 international journals, 5 book series and international conference proceedings and 2 national conference papers. His area of interest in research includes digital image processing, pattern recognition, video analytics, computer vision data analytics, and IoT.

Contributors

Abeebunnisa Sd. EEE Department, Kakatiya Institute of Technology and Science, Warangal, India

Abhishek GB Pant Government Engineering College, New Delhi, India

Agrawal Harshit Department of CSE, National Institute of Technology, Tiruchirappalli, Tamilnadu, India

Ajgarvali Moghal Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

Alam Ashraf Rekhi Centre of Excellence for the Science of Happiness, Indian Institute of Technology Kharagpur, Kharagpur, India

Anuradha T. Department of Information Technology, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India

Ashoka Reddy K. Department of ECE, KITSW, Warangal, India

Babu B. S. S. V. Ramesh Department of ECE, Raghu Institute of Technology, Visakhapatnam, India

Balaji B. Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., India

Bhargava Navneet GB Pant Government Engineering College, New Delhi, India

Butt Muheet Ahmed P.G Department of Computer Science, University of Kashmir, Srinagar, Jammu and Kashmir, India

Chandra Sekhar M. Department of ECE, Kakatiya Institute of Technology and Science, Warangal, T.S, India

Cheerla Sreevardhan Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

Darahasa M. Department of Information Technology, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India

Deepa D. Department of Computer Science and Engineering, Kongu Engineering College, Perundurai, Tamil Nadu, India

Deepanshu GB Pant Government Engineering College, New Delhi, India

Deshmukh Radhika G. Department of Physics, Shri Shivaji Science College Amravati, Amravati, Andra Pradesh, India

Deshwal Manish Department of Electronics and Communication Engineering, Chandigarh University, Gharuan, Punjab, India

Devi Y. Sarada Department of ECE SRM Institute of Science and Technology, Chennai, India

Devika K. D. CRRAO-AIMSCS, University of Hyderabad Campus, Hyderabad, India

Ekka Prachi Medline School of Electronics and Communication Engineering, MIT-WPU, Pune, Maharashtra, India

Ganesh Reddy Electrical Section, Engineering Department, University of Technology and Applied Sciences-IBRI, Ibri, Al Dhahirah, Sultanate of Oman

Govinda Rajulu G. CSE Department, St Martins Engineering College, Secundrabad, Telangana, India

Gunapreetham A. Kakatiya Institute of Technology and Science, Warangal, T.S, India

Gupta Akash Kumar Department of ECE, Centurion University of Technology and Management, Gajapati, Odisha, India;
Department of ECE, Raghu Institute of Technology, Visakhapatnam, India

Hanu Vamshi K. EEE Department, Kakatiya Institute of Technology and Science, Warangal, India

Helini K. Vignan's Institute of Management and Technology for Women, Kondapur, India

Jagtap Vinayak Department of Computer Engineering and Information Technology, College of Engineering, Pune, India

Jamuna Rani M. ECE Department, Sona College of Technology Salem, Salem, Tamil Nadu, India

Jishitha N. Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India

Jyothi Bonagiri Department of Computer Science, Gitam (Deemed to be University), Visakhapatnam, India

Kanakam Ranganath Department of Computer Science and Engineering, Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India

Kishan Rao K. Department of Electronics and Communication Engineering, Srinidhi Institute of Science and Technology, Hyderabad, Telangana, India

Komuraiah B. Department of ECE, KITSW, Warangal, India

Kotaiah Bonthu Department of CS and IT, Maulana Azad National Urdu Central University, Gachibowli, Hyderabad, Telangana, India

Kothandaraman D. School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India

Kulkarni Parag iKnowlation Research Labs Pvt. Ltd, Pune, India

Kumar Durgesh GB Pant Government Engineering College, New Delhi, India

Kumar Nirmalendu GB Pant Government Engineering College, New Delhi, India

Kumar Sandeep GB Pant Government Engineering College, New Delhi, India

Kumar Sanjay GB Pant Government Engineering College, New Delhi, India

Kute Rupali School of Electronics and Communication Engineering, MIT-WPU, Pune, Maharashtra, India

Lakshmi Narayanan S. Department of ECE, National Engineering College, Kovilpatti, India

Lakshmi Ramani B. Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India

Lakshmi V. Naga Department of Computer Science, Gitam (Deemed to be University), Visakhapatnam, India

Mahika Kamale N. Department of Information Technology, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India

Mahitha P. Department of Information Technology, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India

Maithri Yerra CRRAO-AIMSCS, University of Hyderabad Campus, Hyderabad, India

Mamodiya Udit Department of Electrical Engineering, Poornima College of Engineering, Jaipur, Rajasthan, India

Mary G. Aloy Anuja Department of ECE, Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, India

Mohammad Syed Noor Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

Mohammad Sallauddin School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India

Murali K. Department of ECE, Vijaya Engineering College, Vijayawada, India

Nandam Srinivasa Rao Department of Computer Applications, NIT, Tiruchirappalli, India

Narendra Rajashree Dayananda Sagar University, Bengaluru, India

Neeraj Nichenamtela Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

Neha K. Kakatiya Institute of Technology and Science, Warangal, T.S, India

Nirmaladevi R. Department of Electronics and Instrumentation Engineering, KITS Warangal, Warangal, Telangana, India;
Research Scholar, Department of ECE, JNTUH University, Hyderabad, Telangana, India

Nithya B. Department of CSE, National Institute of Technology, Tiruchirappalli, Tamilnadu, India

Panda Sandeep Kumar Department of Computer Science and Engineering, Faculty Science and Technology, ICFAI Foundation for Higher Education, Hyderabad, Telangana, India

Pandey Manish Department of Computer Science and Engineering, Maulana Azad National Institute of Technology, Bhopal, India

Prakash Vodapalli Kakatiya Institute of Technology and Science, Warangal, T.S, India

Prasad N. EEE Department, Kakatiya Institute of Technology and Science, Warangal, India

Prasanth R. Department of ECE, National Engineering College, Kovilpatti, India

Prasuna K. Department of ECE, Vijaya Engineering College, Vijayawada, India

Praveenkumar C. Department of Electrical and Electronics Engineering, Sri Ramakrishna Engineering College, Coimbatore, India

Radhakrishna D. Department of Computer Science and Engineering, N.M.A.M.Institute of Technology, NITTE, Bangalore, India

Raghunandan K. R. Department of Computer Science and Engineering, N.M.A.M.Institute of Technology, NITTE, Bangalore, India

Rajasanthosh Kumar T. Department of Mechanical Engineering, Oriental Institute of Science and Technology, Bhopal, India

Rajendra Prasad P. Vignan's Institute of Management and Technology for Women, Kondapur, India

Rajesh Adepu Department of Computer Science and Engineering, Guru Nanak Institute of Technology, Hyderabad, TS, India

Ramadevi B. Department of ECE, Kakatiya Institute of Technology and Science, Warangal, India

Ramesh Dadi School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India

Ramya N. Department of Information Technology, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India

Ravi Kumar R. School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India

Reddy V. V. Department of ECE, KITSW, Warangal, India

Roopa M. Department of ECE SRM Institute of Science and Technology, Chennai, India

Rupa V. Vignan's Institute of Management and Technology for Women, Kondapur, India

Sagar K. Department of CSE, CBIT, Hyderabad, Telangana, India

Saheb Shaik Himam IcfaiTech (Faculty of Science and Technology), The ICFAI Foundation for Higher Education, Hyderabad, India

Sahu Santosh Kumar Department of Computer Science and Engineering, Maulana Azad National Institute of Technology, Bhopal, India

Sai Varshini B. Kakatiya Institute of Technology and Science, Warangal, T.S, India

Sana Shaik Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India

Saravanan D. Department of Operations and IT, ICFAI Business School (IBS), Hyderabad, The ICFAI Foundation for Higher Education (IFHE) (Deemed to be University u/s 3 of the UGC Act 1956), Hyderabad, India

Satheesh Kumar M. Department of ECE, National Engineering College, Kovilpatti, India

Satish Babu G. Department of Mechanical Engineering, JNTUHCEH, Hyderabad, India

Satish Rama Chowdary P. Department of ECE, Raghu Institute of Technology, Visakhapatnam, India

Saxena Ashutosh CRRAO-AIMSCS, University of Hyderabad Campus, Hyderabad, India;
CMR Technical Campus, Hyderabad, Telangana, India;
C.R. Rao Advanced Institute of Mathematics, Statistics and Computer Science,
Hyderabad, Telangana, India

Shabana Department of Computer Science and Engineering, Sumathi Reddy
Institute of Technology for Women, Warangal, Telangana, India

Sharma Tripti Department of Electronics and Communication Engineering,
Chandigarh University, Gharuan, Punjab, India

Shehloo Arif Ahmad Research Scholar, Mewar University, Chittorgarh,
Rajasthan, India

Sheshikala M. School of Computer Science and Artificial Intelligence, SR Univer-
sity, Warangal, Telangana, India

Shunmugavel S. Department of ECE, National Engineering College, Kovilpatti,
India

Singh Ajeet Acharya Nagarajuna University, Guntur, AP, India;
C.R. Rao Advanced Institute of Mathematics, Statistics and Computer Science,
Hyderabad, Telangana, India

Siron Anita Susan T. Department of CSE, National Institute of Technology,
Tiruchirappalli, Tamilnadu, India

Soma Umamaheshwar Department of ECE, Kakatiya Institute of Technology and
Science, Warangal, India

Sravya T. Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra
Pradesh, India

Sri Durga N. Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada,
Andhra Pradesh, India

Sri Lakshmi T. Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada,
Andhra Pradesh, India

Srinivasa Rao Naarisetti Electrical Section, Engineering Department, University
of Technology and Applied Sciences-IBRI, Ibr, Al Dhahirah, Sultanate of Oman

Srinivas M. EEE Department, Kakatiya Institute of Technology and Science,
Warangal, India

Srinivas M. S. S. S. Department of ECE, Raghu Institute of Technology, Visakha-
patnam, India

Srivastava Saumya Department of Electronics and Communication Engineering,
Chandigarh University, Gharuan, Punjab, India

Srujan Raju K. Department of CSE, CMR Technical Campus, Hyderabad, Telangana, India

Srujay P. EEE Department, Kakatiya Institute of Technology and Science, Warangal, India

Subbareddy V. Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

Sucharitha Inapanuri Department of Information Technology, CBIT, Hyderabad, India

Sultana Shaik Samreen Department of ECE, KITSW, Warangal, T.S, India

Suneel Raja M. Department of ECE, Kakatiya Institute of Technology and Science, Warangal, T.S, India

Suresh E. Department of ECE, Kakatiya Institute of Technology and Science, Warangal, India

Suthendran K. Department of IT, Kalasalingam Academy of Research and Education, Srivilliputhur, India

Swathi A. V. Department of ECE, Raghu Institute of Technology, Visakhapatnam, India

Tagare Trupti Shripad Dayananda Sagar College of Engineering, Bengaluru, India

Tentu Appala Naidu C.R. Rao Advanced Institute of Mathematics, Statistics and Computer Science, Hyderabad, Telangana, India

Thirupathi V. Department of CSE, SR University, Warangal, Telangana, India

Tiwari Vikas Acharya Nagarajuna University, Guntur, AP, India;
C.R. Rao Advanced Institute of Mathematics, Statistics and Computer Science, Hyderabad, Telangana, India

Urkude Shubhangi V. Department of Operations and IT, ICFAI Business School (IBS), Hyderabad, The ICFAI Foundation for Higher Education (IFHE) (Deemed to be University u/s 3 of the UGC Act 1956), Hyderabad, India

Vaddepalli Manoj Kumar School of Computer Science and Artificial Intelligence, SR University, Warangal, TS, India

Vamshi Krishna M. Department of ECE, Dhanekula Institute of Engineering and Technology, Vijayawada, India

Vamshi Adouthu Department of Computer Applications, NIT, Tiruchirappalli, India

Varaprasad Rao M. Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, India

Varaprasada Rao K. Department of Computer Science and Engineering, Faculty Science and Technology, ICFAI Foundation for Higher Education, Hyderabad, Telangana, India

Vijaya A. Department of ECE, KITSW, Warangal, India

Vijitendra Duggirala Department of CSE, National Institute of Technology, Tiruchirappalli, Tamilnadu, India

Vishal G. Kakatiya Institute of Technology and Science, Warangal, T.S, India

Yadav Riya Department of Computer Science and Engineering, Maulana Azad National Institute of Technology, Bhopal, India

Cloud-Based E-learning: Scaffolding the Environment for Adaptive E-learning Ecosystem Based on Cloud Computing Infrastructure



Ashraf Alam 

Abstract The article discusses the top five e-learning technologies that have the potential for substantial growth in the coming years as a result of the growing student population. The current study analyses in brief the efficacy of e-learning services in the classroom and how cloud computing will play a significant role in future of education. While incorporating cloud computing into e-learning services has many advantages, there are certain risks and challenges to consider, including cost, bandwidth, security, user concept, forms, and methods, as well as management duties and resources. Due to the virtualisation of these resources, educational businesses, students, and institutions may also lease them. Cloud computing's autonomous, cost-effective, flexible, and reliable infrastructure enables the creation of an e-learning ecosystem. Cloud-based e-learning systems are much faster, cheaper, and more efficient than on-premises e-learning systems and are considerably safer. Author examined several contemporary technologies and weighed their benefits and drawbacks in this article, concluding that some platforms are there to stay, while others may perish because of its operational difficulty.

Keywords Educational technology · Cloud computing · E-learning · Curriculum · Pedagogy · Cloud-based E-learning systems · Educational administration

1 Introduction

Cloud computing has had a profound effect on computer industry, driving technological progress [1, 2]. With the advent of cloud computing, programmes that were previously delivered via the Internet have undergone significant modifications [3, 4]. Organisations may use this technology to provide services via the Internet [5, 6]. It is a computer architecture that enables users to pay for access to hardware and software resources through a network [7–9]. Cloud computing is currently gaining immense

A. Alam (✉)

Rekhi Centre of Excellence for the Science of Happiness, Indian Institute of Technology
Kharagpur, Kharagpur, India

e-mail: ashraf_alam@kgpian.iitkgp.ac.in

popularity and is a generic term that refers to shared use of virtual resources by several businesses at a facility that distributes computer services [10–12]. Cloud computing may benefit applications with a graphical user interface and server-side applications that are difficult to develop on top of conventional computers and networks [13, 14].

To maintain the present speed of the e-learning system, cloud computing must be used in conjunction with newest multimedia and communication technologies [15, 16]. The current study analyses in brief the efficacy of e-learning services in the classroom and how cloud computing will play a significant role in future of education. While incorporating cloud computing into e-learning services has many advantages, there are certain risks and challenges to consider, including cost, bandwidth, security, user concept, forms, and methods, as well as management duties and resources [11, 12]. Due to the virtualisation of these resources, educational businesses, students, and institutions may also lease them. Cloud computing's autonomous, cost-effective, flexible, and reliable infrastructure enables the creation of an e-learning ecosystem [5, 6].

2 Overview of Cloud Computing

Currently, cloud service consumers expect cloud service providers to offer the following services [4, 5].

Anything-as-a-Service (XAAS): it refers to the delivery of Everything-as-a-Service to anybody, anywhere. This is a word that refers to the manner in which a service is provided.

Infrastructure-as-a-Service (IaaS): Google Compute Engine, Amazon Web Services, and Rackspace are all examples of cloud computing services that provide computer infrastructures in the form of business, network, and virtual machines.

Platform-as-a-Service (PaaS): PaaS is a well-known cloud computing architecture that allows customers to execute their applications without managing any software or hardware infrastructure, such as Google App Engine, Windows Azure, or Force.com.

Software-as-a-Service (SaaS): users of Software-as-a-Service pay a monthly membership fee in exchange for access to application software services. Google Apps, WhatsApp, and Microsoft Office 365 are all examples of services that are unconcerned with programme installation, setup, or operation, since the service provider handles everything.

Storage-as-a-Service (SaaS): stocking is often included as a part of a cloud computing service provider's offering, which enables applications to store both organised and unstructured cloud data. For instance storage is available via the Mozy, Google Drive, and Dropbox services.

Network-as-a-Service (NaaS): cloud computing offers network services to people or companies through the Internet on a pay-per-use or monthly subscription basis, depending on their needs.

Users may choose one or more services based on their specific needs. E-learning services are less expensive to create and operate on a cloud-based platform, and they

provide a wide range of compatibility and flexibility to end users [4–7]. On the other hand, the cloud’s security issues remain unsolved [6, 7].

3 The Implications of Cloud Computing for E-learning

The technological advances in modern information and communication (ICT) technologies heralded a period of unprecedented societal upheaval at the turn of the twentieth century [8, 9]. Cloud computing has emerged as a cutting-edge technology in recent years, accelerating the pace of educational innovation [5–8]. Mobile technologies, authoring tools, digital instructional games, and virtual simulations are only some of the advancements in e-learning technology. The adoption of digital classrooms and the promotion of learner-centered training have created a need for pedagogical design and transformation to suit the requirements of current staff who encourage twenty-first-century skill development via domain knowledge acquisition [2, 5]. Additionally, asynchronous e-learning systems enable users to access and learn from educational resources such as lecture videos and complete assignments at their convenience, rather than at predetermined times and locations. Students may study at their own speed and from any location using e-learning, which is distinct from traditional classroom instruction [4, 6].

The components of cloud-based e-learning architecture may be classified on a number of levels. The infrastructure layer is made up of a collection of scalable and dynamic physical hosts. On the second layer, a standardised interface is accessible to all e-learning developers. At the system level, resource management guarantees the independence of hardware and software resources. The service layer includes a variety of well-known cloud services. Cloud computing services include cloud-based and platform-based software services [2, 4, 12]. Along with administrative and assessment functions, the application layer provides collaboration capabilities such as a virtual laboratory and the ability to share and create content.

A cloud-based e-learning architecture is a subfield of cloud computing that focuses on e-learning systems for the education sector [3, 7, 15]. Students and educational institutions may lease virtualised education resources for e-learning from cloud providers, which they can then rent to other students and educational institutions. A five-tyre architecture for cloud-based e-learning architecture includes: business application layer; server layer; administrative layer; software layer; hardware layer; and network layer [7, 13, 15]. The hardware resource layer is responsible for managing the computer’s fundamental components, such as the CPU and physical memory. This layer of e-learning development is critical to the overall system design. A software resource layer is constructed and supplied with assistance of middleware and operating systems.

4 Methodological Provisions for Rendering Cloud-Based E-learning

It is founded on cognitive science principles and is an excellent method for students to participate in successful multimedia learning through electronic educational materials. E-learning is a time-efficient and cost-effective way of learning that also takes care of user's comfort and the organisation's profit margin [1, 3, 6].

Among the direct and positive effects of e-learning on pupils include improvement of learner-to-teacher ratio on a national and global scale, assisting pupils in learning about a certain programme or subject in a simplified way. Additionally, long-term data and information retention are improved. There will be no out-of-pocket costs on travelling to learning centres [2, 4, 7]. Demand for e-learning thus continues to grow exponentially and is unlikely to slow down in the near future.

5 Vantages of Cloud Computing Adoption for E-learning Solutions

Many educational institutions lack the resources and infrastructure necessary to operate or install an e-learning system. Certain versions of BlackBoard and MOODLE's basic applications, as well as their e-learning tools, are available through cloud-based services. At all levels of education, e-learning is extensively utilised for a variety of reasons, including in-house education, academic courses, and corporate training [1, 3, 6]. Cloud-based e-learning systems provide many advantages over on-premises e-learning systems. Some of which include: the price is competitive, software updates are completed in a matter of seconds, added layer of security for cloud-based e-learning systems enhances overall performance and productivity of employees, enables real-time collaboration among distant team members, revised version is more compatible with document types, and no in-house IT assistance is needed and assists in retaining current employees [9, 13, 16].

There are many benefits for students as well. Pupils can enrol in online distance learning (ODL) programmes. They can send students activities, projects, and tasks from home, can seek feedback, and take examinations at the comfort of their home. Several advantages for educators include: content management, communication with pupils via forums, test preparation, evaluation of tests, grading of students' homework or assignments, projects, and sending of feedback are all included in benefits of e-learning [5, 14, 15].

6 Comparing Different Authoring Tools Based on Cloud Computing

In recent years, e-learning has increased in popularity, with platforms mostly used for human–computer interaction. There are many e-learning products and platforms available today, all vying for learner’s attention and money. Cloud-based authorisation systems are a relatively new and rapidly increasing trend in e-learning [1, 3, 13]. This increasing tendency opens up new opportunities for developing new ideas and methods for editing and proofreading multiscreen courses. This trend is expected to continue. Anyone with access to the Internet and a compatible device, such as a laptop or smartphone, may create virtually any kind of training course using one of the many online educational platforms presently available. Prior to using or sharing any of the goods accessible, a cloud-based e-learning tool should be selected and assessed in comparison to the newest cloud-based learning tools in the market. Numerous contemporary devices have been evaluated, along with their benefits and drawbacks.

6.1 *Easy Generator*

Easy Generator is a complete cloud-based learning platform that enables users to easily create required or requested courses without requiring them to have any coding knowledge. Create learning objectives using the Easy Generator, and encourage instructors to evaluate students’ progress in learning using a sound educational framework. Despite the absence of integrated management tools, students may see their performance and results prior to finishing the course by providing their name and email address.

Easy Generator does not need any scripting or programming skills. It is simple to use. It has the ability to add additional co-authors to fulfil course requirements. Mobile-friendly courses are easy to navigate and use. Due to its simplicity, this next generation authoring tool serves as an excellent example for learning and teaching. It is simple to tailor the questions and responses for appropriate and incorrect feedback. It is straightforward to get started, even without previous expertise or training in educational design or production. It provides website embedding, SCORM, HTML downloads, and private link sharing to make sharing easily possible.

While not shown, the “Academy” plan allows the creation and updating of template material. When a large number of authors need access to the platform, the price becomes prohibitively expensive. For a short time, Easy Generator is available free of charge as part of a freemium model with two basic types. The monthly fee for each author is \$39, but the one with advanced features costs \$59 per month. However, schools get a monthly discount of up to 50%.

6.2 *Lectora Online*

Lectora, a cloud-based online authoring tool, has launched version 2, which includes a number of new features and an improved user interface. Additionally, an evaluation version is available with a 30-day free trial term. Furthermore, tasks may be created for integration with apprenticeship management systems.

Non-subscription access to professional animated films through the Lectora Online Media Library, which eliminates the requirement for a separate membership, as well as the option to download resources such as SCORM, HTML, and Tin Can without the need for members to create a separate account. Each time the course is made accessible, it should be carefully checked to ensure that no errors have been introduced. HTML is neither responsive nor mobile, and its usage does not safeguard sensitive data. For those without interactive features, the majority of these may result in errors. In addition to the \$159 monthly membership price, Lectora charges a \$1908 annual membership fee.

6.3 *eCoach*

eCoach is a relative newcomer to the market for authoring tools, having launched very recently. Anyone can develop new online courses with the help of eCoach, the cross-platform authoring tool that needs no programming expertise. One may create online courses fast and by simply using Internet materials and resources. A no-cost 30-day trial version is available. Numerous templates are accessible, each of which is simple to use and understand. It provides students with access to their material through a course code and a private URL. It has an intuitive and easy-to-navigate user interface. It can fully access educational materials that are mobile-friendly. Students can work in an atmosphere that is aesthetically appealing and well organised. However, because the templates are form-based, new material must be verified before it is published. At the moment, this programme is prohibited from exporting or downloading SCORM or HTML. Teacher membership fees is \$29.95 per month, while subscriptions for all other users are \$49.95 per month.

6.4 *Ruzuku*

Ruzuku is a chess categorisation system that indicates the difficulty of a game. According to the creator, Ruzuku is an authoring tool that is mainly utilised in the classroom as a repository for learning resources. Monitoring all student information is difficult. Users may contribute to the creation of courses by submitting materials, files, and activities that are subsequently shared with other users through the course management system. It offers a 14-day free trial and is one of the three

most user-friendly options currently available in market. The ability to monitor and analyse students' attendance and academic performance data is one of its merits. It enables the creation of registration sites and signup pages, as well as customisation of course registration to meet particular needs. However, courses non-interesting or non-interactive. There are just a few design options available, and there are no previews. Throughout the testing process, the page's loading rate is very slow. Blended learning, short-term courses, seminars, and workshops are all acceptable modes of instruction, but are not purely online. The monthly price is \$49 for up to 25 enrolments; however, unfettered access to all services costs about \$997 per year.

6.5 *iSpring Learn LMS*

iSpring Learn LMS is a cloud-based learning management system that allows the learner to manage courses from almost anywhere. To keep things simple, it provides training and learning organisations with complete control over the solutions they provide to students and workers. If carefully monitored and reported on one's training, one can immediately determine its efficacy. As a course development platform, it is fully extensible and manages the whole e-learning process, including grading students' progress throughout the course. Students may communicate with their instructors and provide comments in real time through a learning management system (LMS). A 30-day trial period during which the programme operates fully unrestricted or modified. It helps create a comprehensive collection of dependable and detailed reports on student's activities and performance.

There are SCORM course providers created by third-party developers. Mobile applications for Android tablets, iPads, and other Apple devices are available for download. Students may save and finish required courses at their convenience, regardless of whether they have access to a computer. The number of courses that a trainer may develop and make accessible for viewing is limitless. iSpring is a good desktop publishing application for both Windows and Macintosh computers. However, if there are many courses, learner will be unable to switch from the tile view and will be forced to go through each one. Individual responses are not retained in SCORM third-party quizzes; only the aggregate score is retained. The Starter Plan costs \$97 per month, while the Pro Plan costs \$197 per month and supports up to 50 or 250 people, respectively. If you have 1000 users, the Enterprise Plan is \$579.00 per month.

7 **Concluding Remarks**

Cloud computing enables on-demand, ubiquitous access to a diverse set of resources that may be rapidly made available to a service provider with little participation or administrative work. Cloud computing includes a number of distinguishing characteristics, including resource availability at any time and from any location, resource

billing based on predefined use metrics, and remote access to computer resources without contacting the service provider. Cloud computing has had a significant impact on the evolution of e-learning. All of the following factors contribute to the success of e-learning: cloud quality, cloud features, institution development, and user readiness.

The article further discusses the top five e-learning technologies that, according to the author, will see substantial growth in the coming years as a result of the growing student population. Every day, the number of e-learners increases at an alarming rate. Educational institutes are progressively examining and focusing on e-learning technologies in order to improve their students' learning abilities. Cloud-based e-learning is being pushed as a legitimate and trustworthy way of teaching by a growing number of companies and educational organisations.

Cloud-based e-learning systems are much faster, cheaper, and more efficient than on-premises e-learning systems, as well as significantly safer. Users do not need cloud-based e-learning or high-end equipment or software to see or share data and hardware with other participants; all they need is an Internet connection. All cloud-based systems undoubtedly have flaws. Author examined several contemporary technologies and weighed their benefits and drawbacks in this article, concluding that some platforms are too difficult to operate.

References

1. Mell P, Grance T (2011) The NIST definition of cloud computing, pp 20–23
2. Pluzhnik E, Nikulchev E (2014) Virtual laboratories in cloud infrastructure of educational institutions. In: 2014 2nd International Conference on Emission Electronics (ICEE), pp 1–3
3. Al-Sharafi MA, Arshah RA, Abu-Shanab EA (2017) Factors influencing the continuous use of cloud computing services in organization level. In: Presented at the 2017 international conference on advances in image processing Bangkok, Thailand
4. García-Peñalvo FJ, Johnson M, Alves GR, Minović M, Conde-González MA (2014) Informal learning recognition through a cloud ecosystem. *Future Gener Comput Syst* 32:282–294
5. Bora UJ, Ahmed M (2013) E-learning using cloud computing. *Int J Sci Modern Eng* 1:9–12
6. Lakshminarayanan R, Kumar B, Raju M (2013) Cloud computing benefits for educational institutions. arXiv preprint [arXiv:1305.2616](https://arxiv.org/abs/1305.2616)
7. Vouk RM, Jararweh Y (2014) The virtual computing lab (vcl): an open source cloud computing solution designed specifically for education and research. *Int J Service Science Manage Eng Technol (IJSSMET)* 5:51–63
8. Al-Sharafi MA, Arshah RA, Abu-Shanab EA (2017) Factors affecting the continuous use of cloud computing services from expert's perspective. In: Presented at the region 10 conference (TENCON), 2017 IEEE, Penang, Malaysia
9. Al-Balushi FM, Bahari M, Rahman AA (2016) Technology, Organizational and Environmental (TOE) factors influencing Enterprise Application Integration (EAI) implementation in Omani government organizations. *Indian J Sci Technol* 9
10. Nguyen TD, Nguyen TM, Pham Q-T, Misra S (2014) Acceptance and use of e-learning based on cloud computing: the role of consumer innovativeness. In: International conference on computational science and its applications, pp 159–174
11. Ibrahim JS (2014) Adoption of cloud computing in higher education institutions in Nigeria, Universiti Utara Malaysia
12. Makoza F (2015) Cloud computing adoption in higher education institutions of Malawi: an exploratory study. *Int J Comput ICT Res* 9

13. Hwang B-N, Huang C-Y, Yang C-L (2016) Determinants and their causal relationships affecting the adoption of cloud computing in science and technology institutions. *Innovation* 18:164–190
14. Sabi HM, Uzoka FME, Langmia K, Njeh FN, Tsuma CK (2017) A cross-country model of contextual factors impacting cloud computing adoption at universities in sub-Saharan Africa. In: *Information systems frontiers*, pp 1–24
15. Alkhater N, Wills G, Walters R (2014) Factors influencing an organisation's intention to adopt cloud computing in Saudi Arabia. In: 2014 IEEE 6th international conference on Cloud Computing Technology and Science (CloudCom), pp 1040–1044
16. Arpaci (2017) Antecedents and consequences of cloud computing adoption in education to achieve knowledge management. *Comput Human Behav* 70:382–390

Web Crawling-Based Search Engine for Programming Languages



Prachi Medline Ekka and Rupali Kute

Abstract A web crawling search engine works on the already existing data found over the Internet. In today's world, people use programming languages as a base for developing software, testing a hardware and simulation of gadgets. Therefore, an engine is required which can find relevant solution links for code errors which will reduce a developer's web browsing time, increase implementation chances and faster production of a software-based project. In this paper through a search engine, solution for errors for programming languages has been tried to be collected in one platform through different sites. The search engine is mainly based on web crawling. There are websites such as Quora, Stack Overflow and GitHub, which gives a solution for a few programming languages, and the search engine will be designed to extract the data from these sites and provide a list of possible answers to the query. Proposed search engine gives better accuracy and faster crawling.

Keywords Search engine · Web crawling · Database · Indexing · Page ranking

1 Introduction

In this century whenever a question arises in a person's mind, let it be scientific or related to any other field, their first instinct is opening a search engine, our answer machine. A search engine can be defined as a program which searches for queries given by the user and tries to find the item or solution from the database, which consists of solution from the World Wide Web. Search engine occupies around ninety-three percent of web traffic. Various studies have shown that about nineteen percent of a developers time is consumed in searching for errors and information while working on a software [1].

P. M. Ekka (✉) · R. Kute

School of Electronics and Communication Engineering, MIT-WPU, Pune, Maharashtra 411038, India

e-mail: ekka.prachi@gmail.com

R. Kute

e-mail: rupali.kute@mitwpu.edu.in

For programming tasks, relevant code examples are often searched by developers [2]. Now there have been several search engines developed in the past and have been optimized since then. Half of the world uses ‘Google’ as their preferred search engine, whereas there are some countries with their own search engines such as South Korea with ‘Naver’, China with ‘Baidu’, etc. Google provides solutions to all the queries which include all the categories; however, through this paper, the solution for a few programming languages will be available on a particular platform.

There are various approaches that can be used to build a search engine. A search engine can also be built in such a way that it can be used for a particular topic of search for example a machine learning based recommendation engine for embedded programmer [3]. Another type of search engine can be an engine which displays the information of a potential job for people who are seeking one according to their interests [4]. The most effective approach is web crawling which is also used by several famous search engines, and it has been proved that it can be further optimized with time for a better performance. In this paper, a web crawler will be used to get the information related to programming languages through various sites. These links will be stored in a database and indexed. Whenever a query will be searched on the search engine, the engine will go through the data stored in the database and will provide the solution.

An approach where the search engine will use data such as crowd knowledge and code snippets is mostly available on public sites [5]. These answers are available but requires a lot of web browsing which may take a lot of the user’s time and effort. Providing all possible answers from various sites in one place can make a developer’s work much easier and faster. And the right keyword used for the crawler can make this search engine much more efficient than browsing for answers on different sites as it will provide all of it in one place. Terms such as web crawling, indexing and ranking are explained in the next section of this paper followed by the literature survey, methodology and conclusion drawn.

2 Web Crawling

A program which browses the World Wide Web to identify web page URLs is known as a web crawler [6]. A web crawler is a very important part of a search engine. A discovery process in which a team of robots (crawlers or spiders) is sent by the search engine to find the updated content or data can be termed as crawling. It also includes indexing. The search engine crawls the web pages and index them. The pages crawled by these crawlers are mostly publicly available pages. The data or content found by these crawlers may vary from images to video to a pdf or csv file, but it still discovers them using the links. The crawler basically looks for a webpage and then follows the links available in those webpages for new links and then keeps it aside for indexing.

When a web crawler crawls through various sites, it collects massive amount of data which is be stored and indexed in the database. Later whenever a query arises, the search engine looks through the database to find the content among the stored

Table 1 Types of crawlers

S. No	Crawlers	Description
1	Universal or Broad Crawler	There is no limitation to these kind of web crawlers, they follow the links to the end and gather all the webpages they come around.
2	Preferential Crawler	This type of crawlers works on the basis of user's interest, the user provides a particular topic which guides the crawler to focus on the webpages related to that topic only [8].
3	Hidden Web Crawler	Hidden Web hides few information behind the query interface which cannot be accessed easily and therefore Hidden Web crawlers deal with these information [9].
4	Mobile Crawler	This crawler reduces network load and selects the required webpages on the server side rather than doing it on the search engine side.
5	Continuous Crawler	Also known as incremental crawler, since the information which has to be retrieved from the internet keeps on changing, this crawler helps to keep the database up to date.

data. The whole process done by a web crawler can be defined as a computer program which browses the whole internet gradually and in an automated way [7]. There are several types of crawlers described briefly in Table 1.

Indexing—The data that the crawler thinks is good enough to serve the queries is stored in the database of contents that have been discovered; this is known indexing. It is a process of placing and analyzing a webpage.

Page Ranking—Whenever a query is raised, the search engine finds all the related webpages and ranks them in order from most relevant to least relevant; this process is called page ranking. The ranking of webpages is done based on a few factors such as the number of times a query word is entered by user and other factors can be decide by the programmer. Since it is not possible for a user to go through all the webpages provided by search engine as output, the page ranking feature of a search engine aligns these webpages on the basis of how relevant they are to user's query [10].

Sqlite3—We needed a database which could be integrated with our Python files, therefore, we have used sqlite3. This database is embedded at the end program and hence used mostly for web browsers. It has a syntax similar to MySQL in Figs. 5 and 6; the values of all tables and urls stored in the database after crawling through its shell can be seen. It also works with PHP which makes it a preferable choice.

3 Literature Review

Sanaya Goel et al. have used data mining to build a search engine for education sector. Web scraping as well as web crawling has been used for the search engine.

Also several crawlers such as Beautiful Soup4 and Urllib request have been used. After the scraping and crawling, the data has been parsed. The crawlers crawl the websites, and the scrappers selectively work on the links made available to them [11]. A PHP-based website with server end processes handled by python programming is made at the end to display the searched query and answer provided by the search engine.

Here Rodrigo Fernandes et al. have paid attention to one of the main problems that occur mostly in a search engine, i.e., the visible gap between the query asked by the user and the information associated with the solution [2]. They have proposed CROKAGE (Crowd Knowledge Answer Generation). Now this tool uses the crowd knowledge to answer the query of the user. They have stored the answers given by several users of Stack Overflow and used that to give the solution of the query. They have also used multi-factor relevance mechanism to decrease the gap problem between the task description and its solution.

F.M. Javed et al. have implemented a web crawler also known as a web spider which browses the web and collects information in a particular manner. After web crawling, the data has been downloaded and stored using a hyperlink procedure. To perform all the above algorithm, the author has used Python. Since search engine's most significant tool is a web crawler, therefore to ensure their databases are up to date, an efficient web crawler has been developed by the author [12].

Since we lack a study which covers the crawling techniques, Manish Kumar et al. in their paper provide a good detail on the available techniques. A conclusion has been drawn from multiple literature surveys available on web crawlers. Different types of crawlers such as universal or broad crawler, preferential crawler, hidden crawler, mobile crawler, etc. and the web crawling policies are discussed by the authors. Also the challenges faced by a crawler, their current status and the performance metrics that can be used has also been discussed. A conclusion has been drawn from this paper that mobile crawler will be used quite frequently in the future [13].

Slamet et al. have proposed a crawler which uses a keyword on which basis the crawler crawls the website related to that keyword only. The keyword is chosen by the programmer such that it covers the queries of the user and provides link related to their queries. Web directories are different from search engines; search engine uses crawlers, whereas the directories are maintained by human editors [14]. The work done here shows that when it comes to terms of time taken and precision, query-based crawlers are more efficient.

Lei Ai et al. have proposed a methodology to develop a search engine for code snippets. They have constructed a database which consists of real-world code snippets. Burrows wheeler transform algorithm has been used for the search. A code statement sequence information-based code snippet recommendation system (SENSORY) has been proposed which recommends code snippets based on the code granularity [15]. Through this approach, the precision and sorting accuracy of the engine have been improved.

4 Methodology

In Fig. 1, the methodology used to build this search engine is described using a flowchart.

4.1 Database

The database for this search engine has been created using sqlite3. This database consists of six tables. The tables are 'Url', 'Word', 'UrlWordLocation', 'Link', 'LinkWords' and 'PageRank'. Among these tables, the main ones are 'Url' and 'Word'. To keep a track of words location, we are using table 'UrlWordLocation'. Also we need to keep a track of links discovered by the crawler and the words that are available with the link, and to do that, we are using tables 'Link' and 'LinkWords'. In Fig. 2, It can be seen how the tables of the database will work.

4.2 Crawling, Indexing and Page Ranking

Two separate Python files are created to access the database and for web crawling. We have used query-based crawler for this search engine. After the sites have been given to the crawler to visit, we will provide a keyword to our crawler. The crawler will crawl the webpage to get all the sites, and when the keyword is provided, it will keep the links related to that keyword only which will later provide the solution to the user's query. The library used by the crawler in this engine is BeautifulSoup4 which helps the scraping of information from the given sites easier. The advantage of

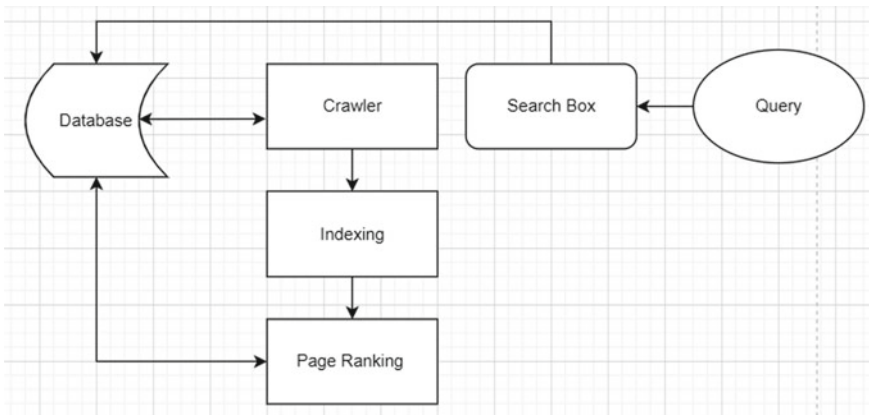


Fig. 1 Flowchart of a search engine

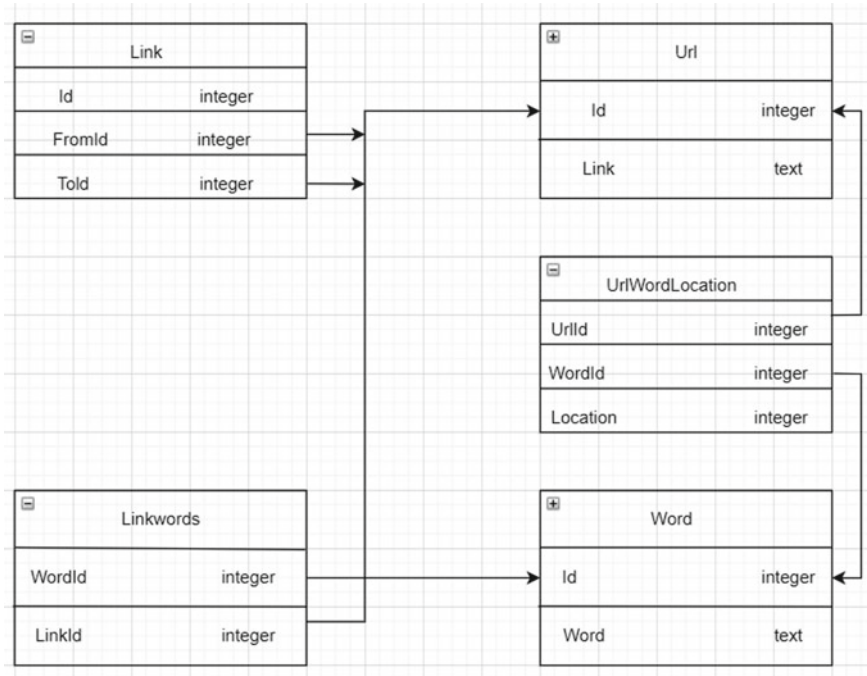


Fig. 2 Block diagram of the database of the search engine

using this library is that it turns out to be quite useful for web scraping as the pages parsed through it can be used to extract data from HTML files easily. The crawler also specifies the path of the database file. It reads all the pages parsed through and returns the soup object of the page content which are the links that can be stored in the database for the engine.

After parsing, the crawler returns all the page URLs with their URL-text. As the crawler crawls through several pages, it continues storing the array of word, word location, URL Id if available and word Id. Since the crawler will keep crawling new websites, it also simultaneously stores the new URLs, words, their Ids and locations in the database. This way the database will remain updated.

The next step is indexing. Crawler also simultaneously keeps indexing the new pages with the old ones in the database for better optimization. The final crawled websites related to the keyword will be stored in the database that has already been created using sqlite3; this process is known as indexing. There is a possibility that even after a keyword is provided to the crawler, it might store a few links which might not be as relevant as other links. Therefore, these links are sorted based on their relevant nature, the links which are more relevant to the query are placed in the beginning, whereas the links which might not be as much relevant are stored at the end, and this process is known as page ranking. This way whenever a query is raised,

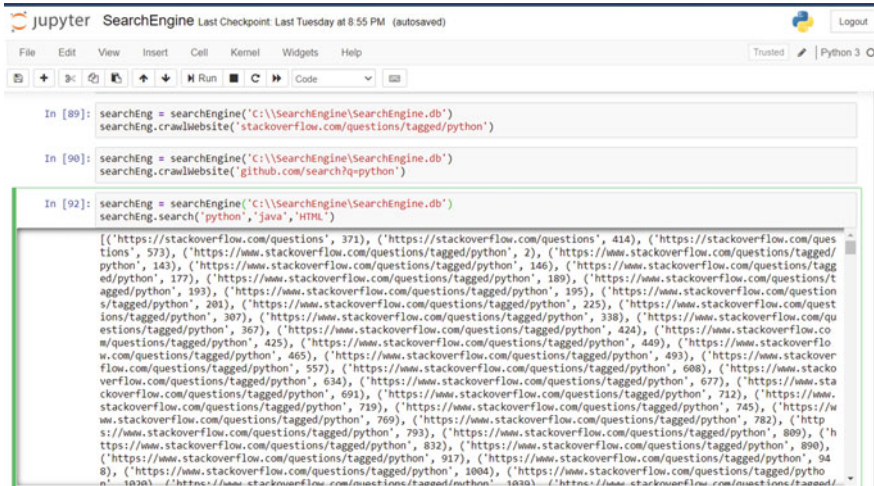


Fig. 3 Results for 'Python, JAVA, HTML' search

the solution to be found in the database will be much easier and it will sort the links according to relevancy in the display for the user.

4.3 Search Engine

A Python-based search engine has been developed to show the working of the crawler and the database together. Figure 3 shows this Python-based search engine and can be further optimized for better functioning. After connecting the search engine to the database, a basic search text can be done at webpages. The entered word by the user will be tried to link with the URLs present in the database. This is why we have used a link word table in the database. After finding the link between the word and the links present in the database, the engine will calculate the page rank of the URLs and the sort those resultant pages according to their ranks for the user. A final website will be created to demonstrate the query and the result of the search engine. This website will also be connected to our sqlite3 database, for which PHP will be used.

5 Results

A search engine that will provide the solutions to a few programming languages has been created through this paper. A query-based crawler has been used or this search engine. In Fig. 3, the image represents the basic working of the engine without PHP or HTML. The search statement in the final line of code represents the search word

```

Command Prompt - sqlite3
.vfsname ?AUX?          Print the name of the VFS stack
.width NUM1 NUM2 ...   Set minimum column widths for columnar output
sqlite> .databases
main: "" r/w
sqlite> .tables
sqlite> .databases
main: "" r/w
sqlite> .databases
main: "" r/w
sqlite> .tables
sqlite> .quit

C:\SearchEngine>sqlites3
'sqlites3' is not recognized as an internal or external command,
operable program or batch file.

C:\SearchEngine>sqlite3
SQLite version 3.35.5 2021-04-19 18:32:05
Enter ".help" for usage hints.
Connected to a transient in-memory database.
Use ".open FILENAME" to reopen on a persistent database.
sqlite> .databases
main: "" r/w
sqlite> .open SearchEngine.db
sqlite> .databases
main: C:\SearchEngine\SearchEngine.db r/w
sqlite> .tables
Link          PageRank      UrlWordLocation
LinkWords     Url           Word
sqlite>

```

Fig. 4 Created tables from the database

entered by the user; in the case below, we have searched for links related to Python, JAVA and HTML, and the box below shows all the crawled relevant links searched by the engine. The result also shows the sites used to scrape the data which are Stack Overflow and GitHub.

In Fig. 4, the tables created inside the database through sqlite3 can be verified, whereas Fig. 5 shows the whether the data has been stored in the database (Fig. 6).

Among the crawled URLs, the ones which are closely related to the question asked by the user will be fetched. As it is visible in above figures that a database and its tables were successfully created. The crawler is also fetching all the keyword-related links through the given sites.

The accuracy of the search engine is calculated using precision, recall and F-score, and the formulas used are given in Table 2.

The mentioned calculated values for three languages in the search engine are given below in Table 3.

For a search engine the metrics precision, recall and F-score determine its efficacy. The proposed search engine overall provides a good precision and recall for the provided languages.

6 Conclusion

The proposed work in this paper is a search engine for programming languages using a query-based web crawler. The main focus of this paper is the crawler since

```

Command Prompt - sqlite3
Error: no such table: SearchEngine
sqlite> SELECT * FROM Link;
1|1|1
2|3|3
3|3|2
4|3|2
5|4|3
6|6|7
7|8|7
8|8|8
9|9|7
10|9|8
11|9|9
12|9|10
13|11|7
14|11|8
15|11|9
16|11|10
17|11|11
18|11|12
19|13|7
20|13|8
21|13|9
22|13|10
23|13|11
24|13|12
25|13|13
26|14|13
27|13|14
28|13|14

Command Prompt - sqlite3
sqlite> SELECT * FROM Linkwords;
9|2
53|3
11|4
12|4
14|5
1201|7
1202|8
1203|9
1098|9
1204|10
1205|10
447|11
448|11
1043|12
343|12
1196|17
1197|18
440|19
1212|19
1883|20
185|20
1883|21
1816|21
1886|21
185|21
185|22
114|23
1257|24
1308|24
1310|24
1257|25
1310|25
1308|25
1975|26
1883|26
1816|26
1886|26
440|26
1458|26
11|26
1204|26
1399|26
317|27
343|27
9|28
448|28
181|29
635|29
2076|29
    
```

Fig. 5 Values stored in the database tables

```

Command Prompt - sqlite3
31 https://www.bh1unt.com/collections/shampoo
32 https://www.stackoverflow.com/questions/tagged/python
33 https://stackoverflow.com/questions/tagged/python?tab=Newest
34 https://stackoverflow.com/questions/tagged/python?tab=Active
35 https://stackoverflow.com/questions/tagged/python?tab=Bounties
36 https://stackoverflow.com/questions/tagged/python?tab=Unanswered
37 https://stackoverflow.com/questions/tagged/python?tab=Frequent
38 https://stackoverflow.com/questions/tagged/python?tab=Votes
39 https://stackoverflow.com/questions/tagged/python
40 https://stackoverflow.com/questions/tagged/python-3.x
41 https://stackoverflow.com/questions/tagged/python-3.x?tab=Newest
42 https://stackoverflow.com/questions/tagged/python-3.x?tab=Active
43 https://stackoverflow.com/questions/tagged/python-3.x?tab=Bounties
44 https://stackoverflow.com/questions/tagged/python-3.x?tab=Unanswered
45 https://stackoverflow.com/questions/tagged/python-3.x?tab=Frequent
46 https://stackoverflow.com/questions/tagged/python-3.x?tab=Votes
47 https://stackoverflow.com/questions/tagged/python-internals
48 https://stackoverflow.com/questions/tagged/python-internals?tab=Newest
49 https://stackoverflow.com/questions/tagged/python-internals?tab=Active
50 https://stackoverflow.com/questions/tagged/python-internals?tab=Unanswered
51 https://stackoverflow.com/questions/tagged/python-internals?tab=Frequent
52 https://stackoverflow.com/questions/tagged/python-internals?tab=Votes
53 https://stackoverflow.com/questions/tagged/python-decorators
54 https://stackoverflow.com/questions/tagged/python-decorators?tab=Newest
55 https://stackoverflow.com/questions/tagged/python-decorators?tab=Active
56 https://stackoverflow.com/questions/tagged/python-decorators?tab=Unanswered
57 https://stackoverflow.com/questions/tagged/python-decorators?tab=Frequent
58 https://stackoverflow.com/questions/tagged/python-decorators?tab=Votes
59 https://stackoverflow.com/questions/tagged/python-dataclasses
60 https://stackoverflow.com/questions/tagged/python-dataclasses?tab=Newest
61 https://stackoverflow.com/questions/tagged/python-dataclasses?tab=Active
62 https://stackoverflow.com/questions/tagged/python-dataclasses?tab=Unanswered
63 https://stackoverflow.com/questions/tagged/python-dataclasses?tab=Frequent
64 https://stackoverflow.com/questions/tagged/python-dataclasses?tab=Votes
65 https://stackoverflow.com/questions/tagged/python-3.7
66 https://stackoverflow.com/questions/tagged/python-3.7?tab=Newest
67 https://stackoverflow.com/questions/tagged/python-3.7?tab=Active
68 https://stackoverflow.com/questions/tagged/python-3.7?tab=Unanswered
69 https://stackoverflow.com/questions/tagged/python-3.7?tab=Frequent
70 https://stackoverflow.com/questions/tagged/python-3.7?tab=Votes
71 https://stackoverflow.com/questions/tagged/python-3.6
72 https://stackoverflow.com/questions/tagged/python-3.6?tab=Newest
73 https://stackoverflow.com/questions/tagged/python-3.6?tab=Active
74 https://stackoverflow.com/questions/tagged/python-3.6?tab=Unanswered
75 https://stackoverflow.com/questions/tagged/python-3.6?tab=Frequent
76 https://stackoverflow.com/questions/tagged/python-3.6?tab=Votes
77 https://stackoverflow.com/questions/tagged/python-import
78 https://stackoverflow.com/questions/tagged/python-import?tab=Newest
79 https://stackoverflow.com/questions/tagged/python-import?tab=Active
80 https://stackoverflow.com/questions/tagged/python-import?tab=Unanswered
    
```

Fig. 6 Crawled URLs stored in the database

Table 2 Formulas of accuracy parameters

S. No	Parameters	Formula
1	Precision	$\text{Precision} = \frac{\text{Number of relevant links retrieved}}{\text{Number of total links retrieved}}$
2	Recall	$\text{Recall} = \frac{\text{Number of relevant links retrieved}}{\text{Number of total relevant links}}$
3	F-Score	$\text{F-Score} = \frac{(2 * \text{Precision} * \text{Recall})}{(\text{Precision} + \text{Recall})}$

Table 3 Search engine evaluation using precision, recall and F-score

S. No	Programming languages	Precision (%)	Recall (%)	F-Score
1	JAVA	75.6	56	0.64
2	Python	98	79.34	0.88
3	HTML	64.61	42	0.50

it does most of the work. An efficient web crawler can discover appropriate links for queries. In this case, the web crawler is quite efficient to travel the webpages that have been given by us. A Python-based search engine is developed to show the basic functioning of the crawler and the engine as well, which shows all the relevant links based on the search. The engine provides a precision of 98%, recall of 79.34% and F-score of 0.88 for Python language when entered a query. Further in Search Engine Optimization (SEO), a more efficient crawler can be developed which would be able to crawl more number of webpages in less time. Since this engine will only work for programming languages, the accuracy will be better and results will be faster. Also the crawler keeps adding new links to its database so that it’s always up to date.

References

1. Rahman MM, Yeasmin S, Roy CK (2014) Towards a context-aware IDE-based meta search engine for recommendation about programming errors and exceptions. In: IEEE conference 2014
2. da Silva RFG, Roy CK, Rahman MM, Schneider KA, Paixao K, de Carvalho Dantas CE, de Almeida Maia M (2020) CROKAGE: effective solution recommendation for programming tasks by leveraging crowd knowledge. In: Springer Science and Business Media,LLc, Part of Springer Nature, 2 Sept 2020
3. Zhou Y, Cui S, Wang Y (2020) Development of machine learning based recommendation engine for embedded programmer. In: IEEE conference 2020
4. Slamet C, Andrain R, Maylawati DS, Suhendar, Darmalaksana W, Ramdhani MA (2017) Web scraping and Naïve Bayes classification for job search engine. In: The 2nd Annual Applied Science and Engineering Conference (AASEC)
5. Ponzanelli L, Bacchelli A, Lanza M (2013) Seahawk: stack overflow in the IDE. In: IEEE conference 2013
6. Zhu H, Xu Y, Fan H, Liu Q (2018) Acceptance evaluation of code recommendation systems by programming behaviors detection and analysis. In: IEEE conference 2018
7. Ahmed TM, Chung M (2018) Design and implementation of an efficient web crawling. In: Proceedings of Korean multimedia society spring conference, vol 21, no 1

8. Pranav A, Chauhan S (2015) Efficient focused web crawling approach for search engine. *Int J Comput Sci Mobile Comput (IJCSMC)* 4(5)
9. Mahar B, Jha CK (2015) A comparative study on web crawling for searching hidden wen. *Int J Comput Sci Informational Technol (IJCSIT)* 6
10. Lavania KK, Jain S, Gupta MK, Sharma N (2013) Google: a case study (web searching and crawling). *Int J Comput Theor Eng* 5(2)
11. Goel S, Bansal M, Srivastava AK, Arora N (2019) Web crawling-based search engine using python. In: *Proceedings of the third International Conference on Electronics Communication and Aerospace Technology (ICECA)*
12. Javed Mehedi Shamrat FM, Tasnim Z, Sazzadur Rahman AKM, Nobel NI, Hosain SA (2020) An effective implementation of web crawling technology to retrieve data from the World Wide Web(Www). *Int J Sci Technol Res* 9(1)
13. Kumar M, Bhatia R, Rattan D (2017) A survey of web crawlers for information retrieval. In: *Wiley Periodicals*
14. Kumar M, Bindal A, Gautam R, Bhatia R (2017) Keyword query based focused web crawler. In: *International Conference on Smart Computing and Communications, ICSCC, 7–8 Dec 2017*
15. Ai L, Huang Z, Li W, Zhou Y, Yu Y (2019) SENSORY: leveraging code statement sequence information for code snippets recommendation. In: *IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*

Smart Helmet for Coal Mine Monitoring



Riya Yadav, Manish Pandey, and Santosh Kumar Sahu

Abstract Since the beginning, coal mining has gained enormous significance with the growing need for energy and has a long history of adverse health impacts on the miners. Underground mining results in suffocation, gas poisoning, object fall, roof collapse, and gas explosion. Therefore, there is a need for an intelligent monitoring system to eliminate these hazards. This paper proposes a smart helmet based on wireless sensor network for real-time monitoring and coal mine safety from the base station. The system provides instant monitoring of hazardous gases like methane, LPG, CO, temperature, and humidity. Falls are the leading contributor to fatal incidents and sometimes the death of miners as appropriate treatment is not provided within the time set. Hence, the proposed system detects a fall and sends the current location of the miner to the base station.

Keywords Underground coal mining · Wireless sensor network · IoT · Sensors · Real-time monitoring system · Fall detection · Accelerometer

1 Introduction

Coal is the primary energy source of many countries in the world. India accounts for 729 million tons of coal resources (as of 2018–2019) and is the second-biggest coal-producing country in the world after China. Coal provides about 50% of India's commercial primary energy supply today and is the dominant fuel for power production. Though the Indian mineral sector has generated employment opportunities and improved livelihoods, it has contributed significantly to environmental degradation. Further, the overall impact of mining is deep-rooted and catastrophic. It has adverse effects on air and water quality, degradation of natural resources, loss of biodiversity, and decrease in rainfall. Apart from this, underground coal mining has played a crucial role in deteriorating the health of miners.

R. Yadav (✉) · M. Pandey · S. K. Sahu
Department of Computer Science and Engineering, Maulana Azad National Institute of
Technology, Bhopal, India
e-mail: riyayadav0210@gmail.com

Numerous accidents occur in a mine, and some miners even die. Therefore, a proper and continuous monitoring system is essential to eliminate these accidents for ensuring safety. The traditional coal mining monitoring system was based on a cable network with several limitations in terms of flexibility, reliability, feasibility, coverage area, and stability. On top of that, data collection was cumbersome and time-consuming via a wired network system. Nowadays, wireless sensor network (WSN) is popularly used for monitoring underground coal mines and has made an appearance as a leading technology [1–3]. Though WSN has strengthened the underground communication system, many mineworkers still adopt manual procedures to monitor the environmental aspects of the underground coal mine. This paper presents a monitoring system based on WSN, which will sow the seed of awareness about the benefits of WSN.

2 System Architecture

2.1 Block Diagram

The entire system architecture consists of a microcontroller that acts as the system's backbone comprising various sensors, as depicted in Fig. 2. The underground coal mine environment contains explosive and toxic gases like carbon dioxide (CO₂), LPG, and carbon monoxide (CO). In addition to this, mines are very dark, and miners might fall unconscious because of suffocation and roof collapse [4]. This might lead to the worker's death if proper treatment is not provided within the time frame. The system provides real-time monitoring of environmental factors like temperature, humidity, hazardous gases existing in the coal mine, and person fall detection. Figure 1 depicts the block architecture of the smart helmet. Different components of the proposed system are briefly discussed below.

2.2 Components

NodeMCU ESP8266 (WSN)

The proposed system uses NodeMCU ESP8266, i.e., Wi-Fi, for transmitting data to the base station. There are various wireless sensor networks like Bluetooth, Zigbee, and Wi-Fi. Though Zigbee provides higher accuracy as its signals penetrate through walls and work effectively in mines, its price is very high and has a short radio transmission range. As far as Bluetooth is concerned, it is not compatible with all devices. The significant advantage of Wi-Fi over Zigbee and Bluetooth is that it can deliver high data rates over large areas to many users (Fig. 2).

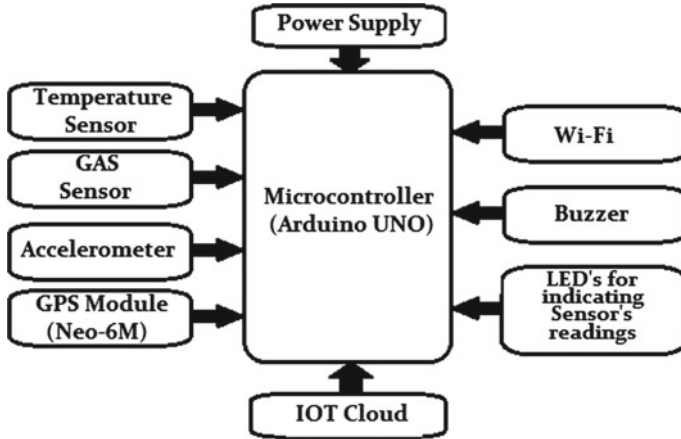


Fig. 1 System architecture

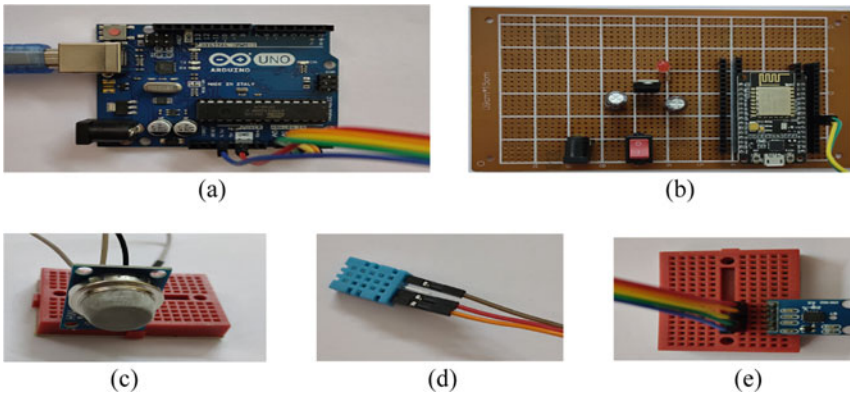


Fig. 2 Components of smart helmet: a Arduino UNO, b NodeMCU ESP8266, c gas sensor, d temperature sensor, and e accelerometer sensor

Gas Sensor (MQ-2)

Gas detector sensors are categorized into three types, i.e., biometric sensor, electrochemical sensor, and metal oxide semiconductor (MOS) sensor. MOS sensor is preferred over other sensors as it is low cost, flexible, easy to use, reliable, has a high life span, and can detect many gases [5]. MQ2 is the wisely used gas sensor in the MQ sensor series.

Temperature Sensor (DHT11)

DHT11 is the commonly used, low-cost temperature and humidity sensor. The working voltage of DHT11 is 5 V DC. It consists of 4 pins and uses only three

pins, i.e., VCC, Data, and GND. It can measure temperature accurately up to $\pm 2^\circ\text{C}$ and can measure humidity accurately up to $\pm 5\%\text{RH}$.

Fall Detection Sensor (ADXL 335)

Fall detection methods are categorized as vision-based approaches using camera, machine learning-based approach, vibrations- and sound-based approach, and kinematic-based approach. In this paper, we have preferred kinematic-based approach to detect a fall as it is portable, easy to use, and relatively cheaper. This approach uses sensors like an accelerometer and gyroscope to analyze whether there has been a fall or not. The proposed helmet uses an ADXL335 accelerometer, which measures acceleration along three axes [6].

GPS Module (NEO-6M)

This module is used to get the coordinates of the miner in the coal mine if he falls and hits the ground [7]. The coordinates are sent to the base station, where the supervisor can view it in Google Map. The system uses NEO-6M for tracking the location. It is a very popular and cost-efficient GPS module. It has an antenna and works well with a power supply between 3 and 5 V.

3 Proposed Methodology

The proposed system incorporates five preeminent modules, (1) Temperature module, (2) Gas module, (3) ADXL335 accelerometer, (4) NEO-6M GPS module, (5) Wi-Fi module, all integrated as one system. The sensors continuously transmit the data to the base station via Wi-Fi. The data received via WSN is uploaded to the cloud, where it can be analyzed and visualized using the ThingSpeak platform [8]. Figure 3 illustrates the flowchart of the proposed algorithm.

4 Experimental Result and Analysis

The result presented in this section is related to the testing we performed on the helmet. We conducted some tests on the system to check the integrity and functioning of the proposed approach which are discussed below. Figure 4 shows the final prototype of the implemented smart helmet.

4.1 Temperature and Air Quality Test

A threshold has been set prior for both MQ-2 and DHT11 sensors for determining the sensor reading. Once the sensor's reading exceeds the threshold level, a green LED

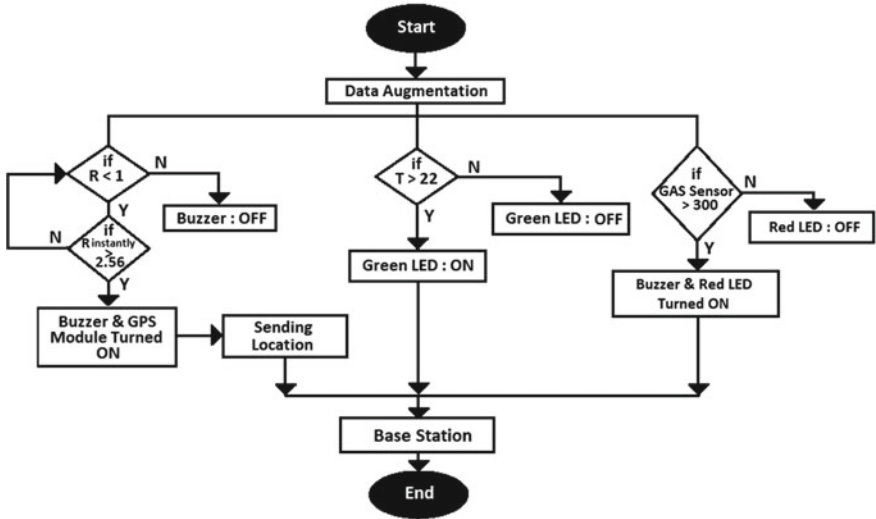


Fig. 3 Flowchart

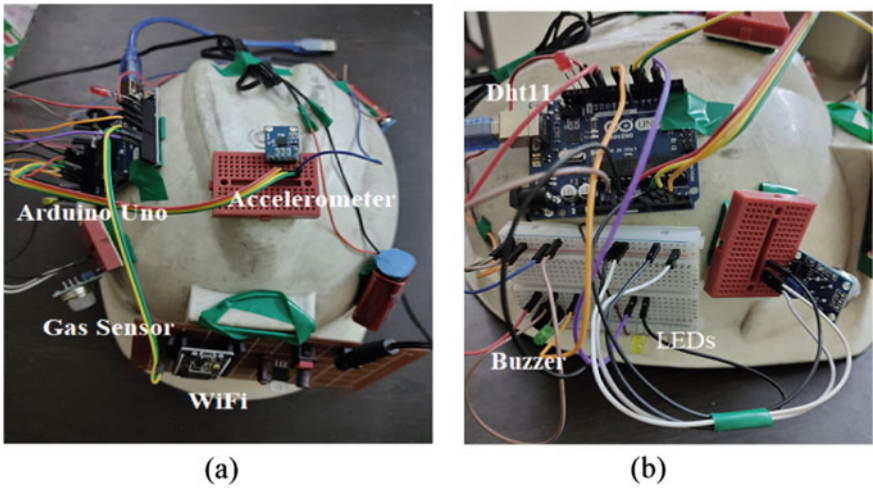


Fig. 4 Prototype of smart helmet. a and b show the system from different angle

turns ON, indicating increased temperature. Red LED turns ON for exceeding the gas level, and at the same time, buzzer is set ON. Then, the data is sent and analyzed at the base station using ThingSpeak. Figure 5 shows how temperature, humidity, and gas concentration varied on a particular day.

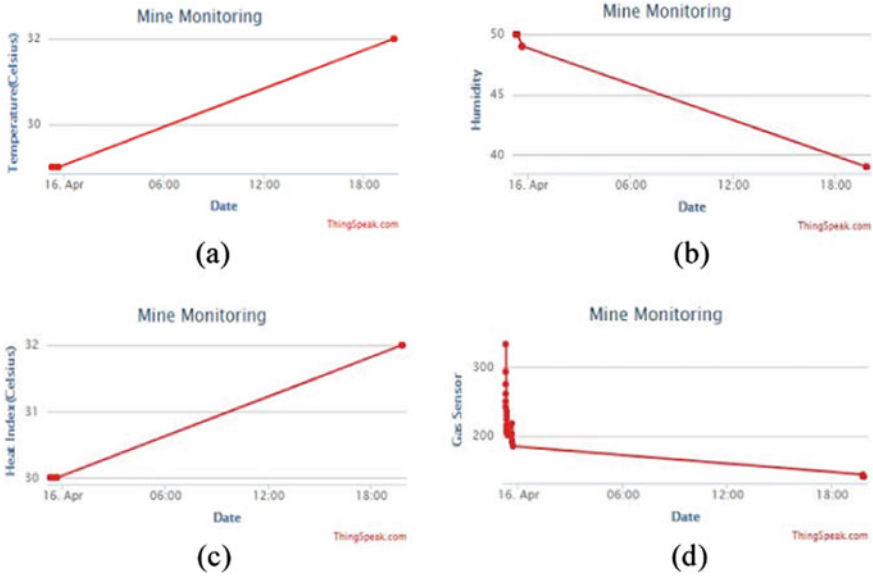


Fig. 5 ThingSpeak data analysis: **a** temperature reading, **b** humidity reading, **c** heat index, and **d** gas sensor reading

4.2 Fall Detection Test

ADXL335 accelerometer module transmits data about the fall of a person to the base station. It is connected to the Arduino UNO, which converts the sensor's analog output into digital output ranging from 0 to 1023 [9]. These values are then converted into equivalent 'g' values in all axes using the below equation:

$$X = \frac{\frac{Val_x - VCC}{1024} - 1.5}{Se} g \quad (1)$$

where

- X = Respective Value along X -axis in g 's
- Val_x = Measured ADC value along x -axis
- VCC = Input voltage applied to the accelerometer
- Se = sensitivity scale factor of ADXL 335 = 0.33.

These equivalent 'g' values along the three axes are then used to find the resultant value using the equation below.

$$R = \sqrt{X^2 + Y^2 + Z^2} g \quad (2)$$

where X, Y, Z are the equivalent ‘g’ values corresponding to $x-, y-, z$ -axes, respectively, and R represents the resultant gravitational acceleration used to detect the fall. This value changes when a person or a body falls and is substantially higher than 1 g when the person is walking, running, sitting, etc. [10]. There is a only single instance in which the resultant (R) is less than 1 g, i.e., during free fall. When a person falls, the resultant value will be between 0 and 1 g and will spike to a considerable value as soon as it hits the ground.

Our method uses the above methodology to detect a fall. The accelerometer continuously measures the values in all directions, and the resultant is calculated. If, at any time, the value of g is below 1 g, the algorithm waits until it encounters a sudden increase in the resultant due to the impact with the ground and calls the GPS module, which in turn sends the coordinates of the fallen person to the base station. Simultaneously, the buzzer gets ON, which alerts the people in the closed vicinity, and immediate help can be provided. The coordinates of the location can be viewed in Google Map as shown in Fig. 6.

Fig. 6 Location details viewed through Google Map

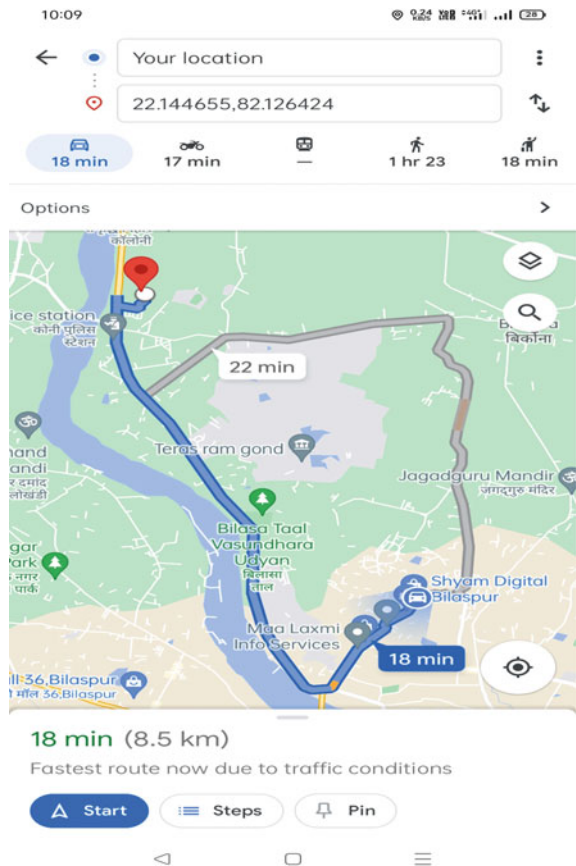


Table 1 Accelerometer values for different activities

S. No	Activity	Accelerometer Resultant value (R) in 'g'
1	Walking (at regular speed)	1.32
2	Walking (fast)	2.19
3	Sitting (at regular speed)	1.68
4	Sitting (fast)	2.12
5	Free fall	Less than 1
6	On impact after Free fall	Greater than 2.56

The above algorithm was tested in different scenarios, which resulted in different 'g' values, as shown in Table 1.

5 Conclusion and Future Scope

The proposed system is a novel approach for monitoring underground coal mines. The system was developed by keeping in mind the needs of coal miners. The components used in the system are cheap, convenient to use, and readily available. The incorporation of the IoT paradigm in mine has enabled each object of the mine to communicate to the Internet. IoT is used as a tool for achieving cost optimization and improving safety measures. The smart helmet is capable of detecting the environmental conditions of the coal mine. The experimental results show that the helmet is efficient in detecting falls.

In the future, we plan to optimize the system by improving the reliability of the proposed approach. We will develop a group of interconnected networks and enhance the existing framework by exploiting more advanced and progressed sensors to determine the risks involved underground. We will try to test the fall detection algorithm on different age groups and consider more testing activities.

References

1. Muduli L, Mishra DP, Jana PK (2018) Application of wireless sensor network for environmental monitoring in underground coal mines: a systematic review. *J Netw Comput Appl* 10:48–67
2. Chen W, Wang X (2020) Coal mine safety intelligent monitoring based on wireless sensor network. *IEEE Sensors*
3. Zhu Y, You G (2019) Monitoring system for coal mine safety based on wireless sensor network, *IEEE* 2019
4. Deokar SR, Kulkarni VM, Wakode JS (2017) Smart helmet for coal mines safety monitoring and alerting. *IJARCCCE* 6
5. Barsan N, Koziej D, Weimar U (2007) Metal oxide-based gas sensor research: how to. *Sensors Actuators B: Chem* 125:18–35

6. Gharghan SK, Nordin R, Ismail M (2016) Energy efficiency of ultra-low-power bicycle wireless sensor networks based on a combination of power reduction techniques. *J Sensors* 2016:21
7. Hema LK, Indumathi R, Prabhakaran, Kumari D (2021) Handheld tourist guidance system using GPS. In: *Materials today: proceedings*
8. Gopal BVSP, Akash P, Aruna Sri PSG (2019) Design of Iot based coal mine safety system using Nodemcu. *IJITEE* 8(6)
9. Ali Hashim H, Mohammed SL, Gharghan SK (2020) Accurate fall detection for patients with Parkinson's disease based on a data event algorithm and wireless sensor nodes. *Measurement*
10. Hariharan A, Sourab S, Varshini VS, Rajpal I, George SM (2019) Remote fall detection system for the elderly. In: *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICT)*

K-Weighted Cluster Head Selection in Wireless Sensor Networks



T. Siron Anita Susan, B. Nithya, Harshit Agrawal, and Duggirala Vijitendra

Abstract Wireless Sensor Networks (WSNs) are emerging technologies with a huge range of potential applications. They are different from other wireless technologies due to a set of specific requirements and feature such as node density, power requirements, and computer capabilities. To increase the lifetime of WSN, clustering is one of the most important ways which includes the collection of sensor nodes into groups and the selection of Cluster Heads (CHs) for each clusters. This paper focuses on hierarchical cluster head selection that aims to reduce the number of dead nodes in WSN. To attain this, K-Weighted Cluster Head Selection (K-WCH) algorithm is proposed with a weight factor to reduce the computational overhead. The proposed algorithm prolongs the network lifetime by reducing the computational energy and minimizing the number of dead nodes. From the simulation results, it is inferred that the proposed K-WCH algorithm outperforms K-means and LEACH protocol in terms of energy consumption and dead nodes.

Keywords Wireless sensor network (WSN) · Clustering · Cluster head · Network lifetime · K-means algorithm · LEACH · Energy consumption

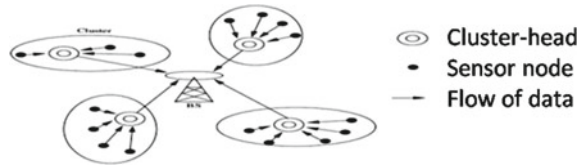
1 Introduction

WSN [1] is a wireless organization that comprises disseminated free nodes utilizing sensors to screen the physical or natural conditions, for example, temperature, sound, vibration, pressure, movement, at various areas. Apart from military applications, it is utilized in numerous non-military personnel application regions, including climate, medical care applications, home computerization, and traffic signals. It has large numbers of sensors where every single hub is associated with one another. Sensor

T. Siron Anita Susan (✉) · B. Nithya · H. Agrawal · D. Vijitendra
Department of CSE, National Institute of Technology, Tiruchirappalli, Tamilnadu, India
e-mail: anitasusan.t@gmail.com

B. Nithya
e-mail: nithya@nitt.edu

Fig. 1 WSN clustering



hub is associated with a focal spot called a base station that gives an association with the world.

The sensor node is rigged with detection aids and computing system, radio transceivers and power components. These sensor nodes are restricted to unsustainable resources, limited operating speed, less storage capacity, and minimum network bandwidth. They may be afflicted with limited reliability, low service level (e.g., high delay, high variability, high independent loss), and security exposure (e.g., service rejection, overcrowding, disruption, high error values). They are responsible for setting up their own appropriate network infrastructure through multi-hop communication and forms clusters if needed. The sensors collect information that is of interest to them and also respond to queries sent from the base station or sink for specific commands and provide relevant data. Thus, the operating mode of the sensor nodes can be continuous or operated by an event. Global Positioning System (GPS) and positioning algorithms are utilized to locate and store location information.

Clustering is a basic mission in WSN for energy effectiveness and organization consistency as it is able to tackle numerous issues like adaptability, energy, and lifetime issues. The large sized WSN is divided into number of clusters, and each cluster is controlled by Cluster Head (CH). CH monitors and controls the data transmission within the cluster. Also, it aggregates the data from CHs and transfers it to the sink node or Base Station (BS) as shown in Fig. 1. The process of re-selection and re-grouping of efficient cluster heads is also necessary thus increasing the lifetime of the network. The cluster heads can likewise shape another layer of clusters among themselves prior to arriving at the sink. Clustering increases scalability and gives logical organization of small cluster which is simple to manage. Moreover, clustering of network also helps in efficient dynamic routing of sensor nodes and is extensive in energy conservation.

Ruthranath et al. [2] categorized the cluster formation into four categories: (1) *Heuristic clustering*—where clusters are formed based on a specific metric in a tree format until some cut off is provided. Some of the examples are linked cluster algorithm (LCA) [3], max-min cluster algorithm [ref], etc. (2) *Weighted schemes*—This is a relatively new algorithm that aims to find a long-lasting architecture like the weighted clustering algorithm (WCA) [4] and reconfigures only when it is absolutely necessary. (3) *Hierarchical algorithms*—This is used when the clusters are merged iteratively until all the elements belong to one single cluster. It is the most straightforward and popular among all the other categories. Example: LEACH [5] protocol, energy-efficient clustering scheme (EECS) [3], Two-Level LEACH (TL-LEACH) [6], hybrid energy-efficient distributed clustering (HEED), etc. (4) *Grid schemes*—These algorithms try to form cluster grids based on the cluster heads for more efficient

queries and data transfer. Example: Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [6].

The popular unsupervised hierarchical Low-Energy Adaptive Clustering Hierarchy (LEACH) [5] is a time division multiple access (TDMA)-based MAC protocol which aims to reduce the energy dissipation among all nodes, thus improving the network lifetime significantly. LEACH takes a systematic way and constructs nodes into clusters. CH sets the TDMA schedule and transfers it to all nodes in its cluster. In addition, the system can be used by locations to determine the time gaps in which they should operate. This allows the node of each group, with the exception of the main cluster head, to turn off its radio components until it is allotted time. It is a probability-based model. Here, the selection of CH is semi-random, and it is based on the percentage of maximum cluster heads and the last chance of CH. By doing so, the energy dissipation is spread across the network instead of draining only for a few CHs.

The random selection of clustering of LEACH results in uneven CHs and the data which are buffered in the dead CHs become useless without reaching the destination. Our proposed K-WCH overcomes the problem of uneven CH selection thereby reducing the dead CHs. Also, the remaining energy of the node is not considered in LEACH while electing the CH. Our K-WCH algorithms concentrated more on residual energy on CH selection to increase the lifetime of the network. The rest of the paper is structure as follow. In Sect. 2, related work is briefly explained. Section 3 gives the proposed K-WCH algorithm, and finally, Sect. 4 provides the result comparison and conclusion of the paper.

2 Related Work

Clustering deals with the problem of grouping of nodes. Clustering in sensor network is significant to tackle numerous problems of adaptability, energy, and lifetime of the network. This clustering mainly focuses on efficient CH selection by using various factors for selection.

Sahanji et al. [7] divided each round of LEACH algorithm into two phases as *setup phase and steady phase*. In setup phase, every sensor node selects a randomly generated number between 0 and 1. If the sensor node picks the number which is lesser than the threshold value, then that sensor node becomes a cluster head. In steady phase, the actual data transmission between the nodes and the cluster heads and between the cluster heads and the base station is performed. This data transfer is based on the TDMA schedule. The cluster heads that receive information from the nodes perform data fusion/aggregation using its local processing resources and send the relevant compressed information further to the BS.

Chung et al. [8] discussed some of the famous clustering algorithms with machine learning concepts. They considered the nodes to be “points” in an N-dimensional space with the Euclidean distance as the distance metric between points. Agglomerative hierarchical clustering algorithm is proposed, where each individual data point

is assumed to be a single cluster. It initially calculates the proximity matrix. Then the two closest clusters are merged and recalculate the proximity matrix, and the merging is done until there is only one cluster remaining.

Rabia et al. [9] addresses the random cluster head selection protocol in conjunction with the cost of hierarchical power range of the wireless sensor network. The basic model based on the LEACH protocol is redesigned to calculate power consumption in three phases of data transfer from the sensor nodes to the sink. It is shown that this model depletes more than 20% of the network capacity in data transfer. It has the disadvantage of not considering energy-efficient CHs.

Fuzzy C-means [10] is a form of clustering where each data point belongs to more than one cluster. This is called soft clustering based on unsupervised learning. The algorithm assigns membership to each data point and nearer the data point to centroid gets more membership. After each iteration, the centroid and membership of data points were updated. FCM algorithm is comparatively better than K-means clustering algorithm. Hoang et al. [11] proposed the cluster head selection based on this *fuzzy C-means*. The algorithm initially chooses the number of clusters and assigns coefficients randomly to each data point in the clusters. For each data point, its coefficients are computed and the entire process is repeated until the algorithm has converged. The convergence happens when the threshold value is attained based on the difference in coefficients or when max iterations achieved. Once the clusters are formed, CH is chosen based on the residual energy of the node in each cluster.

Shengchao et al. [12] proposed a mechanism to model the fuzzy partition of the nodes as clusters. The CH is selected based on the node's density and the distance between each node, and the CH is taken as the weight for the membership. Initially, optimum number of CHs are estimated based on the energy consumption of data fusion and data collection (gathering). Then the centroids are initialized for the matrix, and a new classification matrix is constructed to form clusters. The CH selection is based on the residual energy of candidate nodes of each cluster. The matrix construction makes the data communication cheaper but quiet complex.

Dhirendra et al. [13, 14] proposed distance-based hierarchical clustering where the network is divided as a square grids by the BS, and these grids are termed as clusters. The information of corresponding sensor nodes of each cluster is broadcasted to BS. The residual energy and the distance factors are calculated by BS. Then the BS selects the CH of each cluster based on maximum energy distance factor. In next round, this factor is calculated by the present CH of that cluster, and the CH will discard its head quality once new optimal CH of that cluster is chosen. The division of the grid only decides the size of the cluster and the number of neighbors of the CH and its members. Selection of CH for an empty grid is inefficient. Pawan et al. [15] proposed the clustering where the sensor nodes are randomly distributed in a square grid of same size. The center of cluster is calculated based on the center of gravity of grid and the sensors of the cluster. The quality of the cluster is calculated based on entropy criteria, densities of intra and inter-cluster which is take one major factor to select the CH. The CH of each cluster is then chosen using fuzzy logic with parameters like energy per cluster, residual energy of sensors, distance factor, cluster quality, and cluster density. The process of calculating cluster quality is complex.

2.1 Overall Inference and Motivation

From the above discussion, it is inferred that clustering is needed to manage a huge count of nodes. Sensor nodes are more inclined to failure and energy loss so the clustering should be carried out efficiently to increase the network lifetime by decreasing the dead nodes. The foresaid algorithms rely on clustering which mainly focus on only the residual energy or the distance of transmission. A CH communicates with in neighborhood which is the major source for energy drain of that CH, so larger number the neighbor nodes, the larger is the energy loss. So the CH selection should also consider the number of neighbors to select the CH of the cluster. Also, the fore-said algorithms have not considered this weight factor for CH selection. Weighted clustering helps to assign more significance to nodes with higher weights and clusters are made in accordance with both the weights and distances of the nodes.

3 Proposed K-weighted Cluster Head Selection (K-WCH) Algorithm

Clustering with K-means [16] is an unsupervised learning method which means that the model will itself have to recognize and form patterns from the given data. Weighted K-means clustering [11] is to achieve the motive of considering nodes that have higher energy to become the cluster heads, thereby achieving a better distribution of energy. However, the proposed K-WCH algorithm optimizes the CH selection based on the run time measurements such as distances, residual energy, and neighborhood for a greater lifetime of the WSN nodes and is shown in Algorithm 1. With these network status indication parameters, the proposed K-WCH algorithm calculates the weight factor and elects a node with the higher weight and residual energy as a CH.

Initially, the BS of the network (N_i) gathers the location information of all its nodes and calculates the distance vector of all nodes. The calculated vectors were stored in a matrix for all pair of nodes. It also collects the residual energy levels of the nodes. This node information is maintained by the BS, and with this collected information, it calculates the optimal number of clusters for the network. The number of clusters was defined in Eq. 1 as of [16]

$$num_clust = \frac{\sqrt{len(i)}}{\sqrt{2*3.14}} \quad (1)$$

where i is the total number of nodes and $len(i)$ gives the size of network.

Each node of the network calculates its corresponding neighbor area by dividing network size (M) with a constant factor 10 [ref]. Once the neighboring area is determined, the number of nodes in that area is also estimated. With these collected information, the weight factor of K-WCH is calculated using the proposed Eq. 2.

$$weight_fact = \frac{(E_res * Ne)}{Dist} \quad (2)$$

where E_res is the residual energy of the node, Ne is number of neighbors, and $Dist$ gives the distance between the node and BS. Now, the clustering is performed using the weighted K-means algorithm. Based on the calculated weight factor, the clustering happens by choosing the highest weight factor to cluster the members of the network. Once the cluster where formed the node with the highest residual energy is chosen as the cluster head.

The cluster heads that receive the packets perform data aggregation and then send the relevant compressed information further to BS. The data transmission between the nodes and the cluster heads and also between the cluster heads and BS consumes energy which needs to be calculated for every iteration. Each iteration, the energy drop experienced by the members of the cluster (E_dropM) and CH node (E_drop) is calculated, respectively, by Eqs. 3 and 4

$$E_dropM = l * E_tran + l * E_fsm * min_dist^2 \quad (3)$$

$$E_drop = l * E_trans + l * E_ad + l * E_tran + l * E_mpf * Dis_BS^4 \quad (4)$$

where l is message size in bits, min_dist is the distance between node and its corresponding CH, E_fsm is the energy taken to transmit 1 bit of data in free space model, E_mpf is the energy taken to transmit 1 bit of data in multi-path fading model and M is the size of network (diameter), E_tran is energy taken to operate the transceiver and E_ad is the energy for data aggregation.

Algorithm 1 K-Weighted cluster head selection (K-WCH)

	Input: Initial network (N), Network_size (M), Initial energy ($E_initial$)
	Output: Cluster C_i , Cluster head CH_i
1	Procedure <i>CH_setup()</i>
2	Initialization of Network N_i then Select a BS,
3	BS calculate and store Res_eng and distances of each node
4	Calculate the num_Clust as of Eq. 1
5	For each N_i
6	calculate the neighborhood as $Neighbour_area = M/10$
7	res Matrix store distance of all pair of nodes
8	Neighbourarraygeneration
9	End
10	For each N_i
11	Calculate the $weight_fact$ as in Eq. 2
12	End
13	Repeat clustering with $weight_fact$ until $CH(i) = num_clust$

(continued)

(continued)

Algorithm 1 K-Weighted cluster head selection (K-WCH)		
14	For each CH	
15		Choose Max weight_fact as Chi
16	End	
17	Procedure Transmission()	
18	Initiate TDMA packet transmission between the Ni and CHi and between the CHi and the BS	
19	CH perform data aggregation on transmission	
20	For each member of Chi	
21		Calculate E_dropM as in Eq. 3
22	End	
23	For eachChi	
24		Calculate E_drop as in Eq. 4
	End	

4 Simulation and Performance Analysis

The clustering is carried out in Python 3.9.7 with Numpy and SKlearnlibraries. The simulation is conducted by MATLAB R2016b on an Intel (R) core (TM) i7-6700 CPU with 3.40 GHz and 16 GB RAM. Each sensor node transmits a 4000 bit message to the CH at each round. The other simulation setup details are shown in Table 1.

Table 1 Simulation parameters

Parameter	Symbol	Value
Sensor area	$m \times m$	450 m \times 450 m
Base station	(x, y)	(225, 225)
Number of nodes	Ni	200
Data aggregation energy	E_ad	5 nJ/bit
Initial energy	E_initial	0.2 J/node
Energy for transceiver circuit	E_trans	50 nJ/bit
Energy in free space model	E_fsm	10 pJ/bit/m ²
Energy in multi-path fading model	E_mpf	0.0013 pJ/bit/m ²

4.1 Reaching 10% of Dead Nodes

This parameter shows the relationship between 10% of dead node and number of iterations required for that. From the Fig. 2, it is inferred that the proposed K-WCH has 10% of dead node only after reaching 180-th iteration. Whereas in LEACH, 10% of nodes are dead after 100-th iteration, and in K-means, it is around 160. This reveals that the proposed K-WCH algorithm prolongs the network lifetime by extending the life of the nodes there by conserving the energy to avoid earlier dead nodes. Moreover, the number of dead nodes with respect to number of iterations is also plotted in Fig. 3. Up to 62 iterations, no dead nodes are identified by any of the algorithms. In the proposed K-WCH, the first dead node is reported only at iteration around 100. Though K-means has first dead node around 110-th iteration, the number of dead nodes is increased in the following iterations.

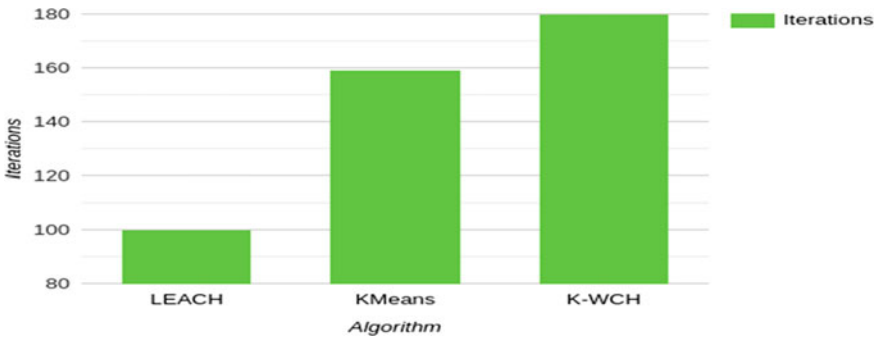


Fig. 2 Reaching 10% of dead nodes

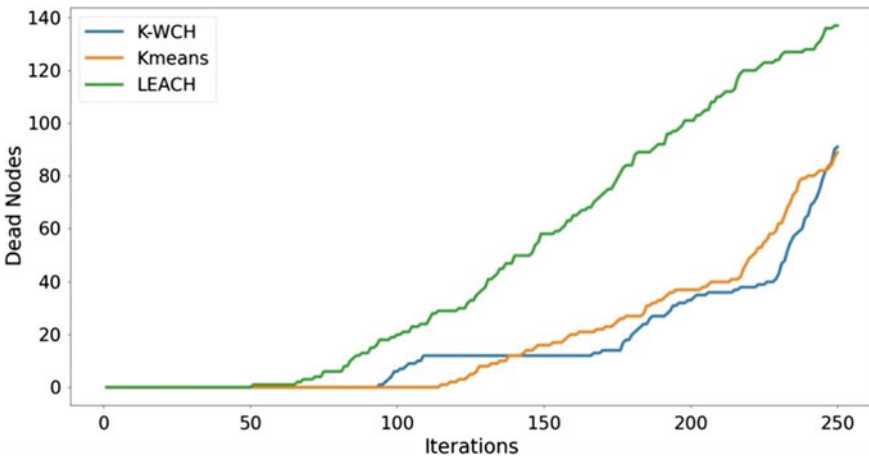


Fig. 3 Number of iteration versus number of dead nodes

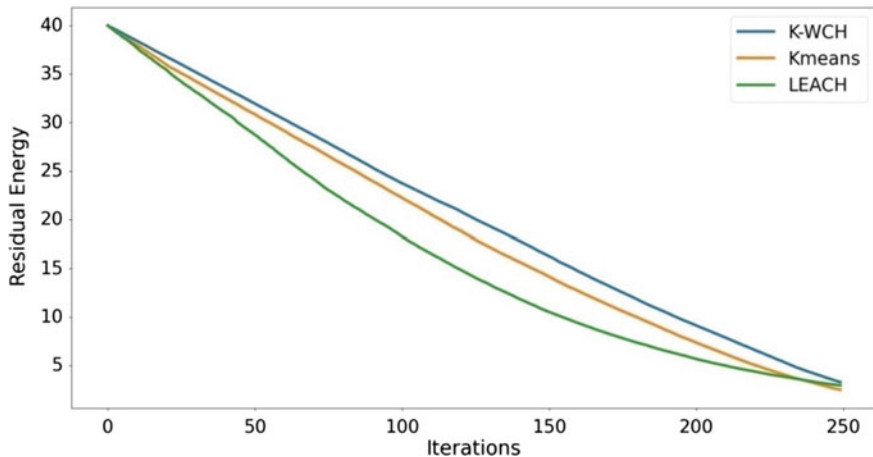


Fig. 4 No. of iteration versus sum of energy

4.2 Energy Efficiency

Figure 4 shows the remaining energy of the network after each iterations. The proposed K-WCH algorithm shows that the residual energy seems to be higher than the other two algorithms. As mentioned in the previous section, the proposed algorithm has more number of alive nodes than other two algorithms. Consequently, the total amount of remaining energy in the network is high. Whereas in other two algorithms, only lesser number of alive nodes participate in the communication thus reducing residual energy of the network.

In Fig. 5, the energy drop after each iteration is plotted for the three algorithms. For LEACH, the energy consumption after 150 iteration is less. Since most of the nodes are dead, there are only lesser number of active nodes thus consuming lesser energy. As opposed to this, the proposed algorithm consumes more energy after 200 iterations due to more of alive nodes.

5 Conclusion

Traditional WSNs are evolving with different clustering algorithm to enhance the overall performance of the network. From the literature review, it is observed that the residual energy and distance are not sufficient to construct the cluster, but also the other parameters like longevity, quality of service, transmission rate, scalability, etc. need to be considered. With these run time parameters, K-WCH is proposed to optimize the selection of cluster heads in the setup phase of LEACH protocol. The simulated results reveal that the proposed K-WCH algorithm is more efficient than K-means and LEACH in terms of energy conservation and longevity. In future, the

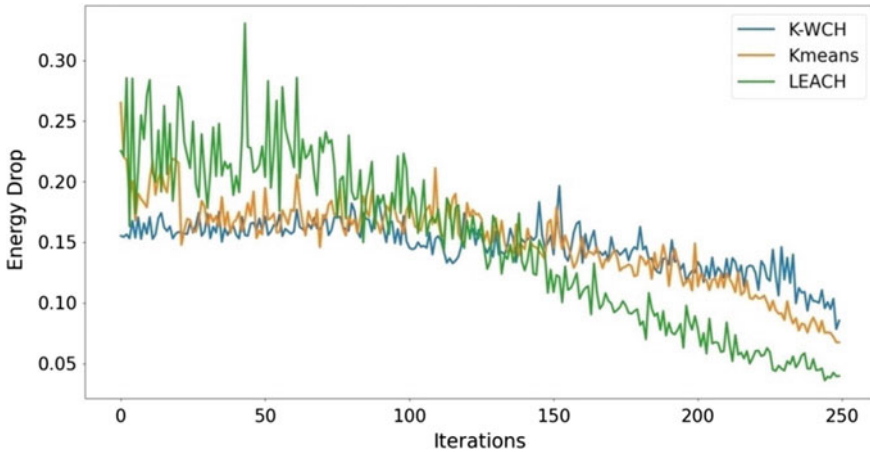


Fig. 5 No. of iteration versus energy drop

optimal route selection with the elected CH can be proposed for the reliable data transmissions in WSN.

References

1. Shahraki A, Taherkordi A, Haugen Ø, Eliassen F (2020) Clustering objectives in wireless sensor networks: a survey and research direction analysis. *J Comp Net* 180
2. Mitra R, Nandy D (2012) A survey on clustering techniques for wireless sensor network. *Int J Res Comp Sci* 2:51–57
3. Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E (2002) A survey on sensor networks. *IEEE Commun Mag* 40:102–114
4. Warneke B, Last M, Liebowitz B, Kristofer, Pister S (2001) Smart dust: communicating with a cubic-millimeter computer. *Comput Mag* 34:44–51
5. Kalkha H, Satori H, Satori K (2016) Performance evaluation of AODV and LEACH routing protocol. In: *Advances in information technology : theory and application*, pp 2489–2703
6. Meyer S, Rakotonirainy A (2003) A survey of research on context-aware homes. In: *Workshop on wearable, invisible, context-aware, ambient, pervasive and ubiquitous computing*, vol 21
7. Sanhaji F, Satori H, Satori K (2017) Clustering based on neural networks in wireless sensor networks. In: *Proceedings of international conference on computing and wireless communication systems*, 19
8. Lung C-H, Zhou C (2010) Using hierarchical agglomerative clustering in wireless sensor networks: an energy-efficient and flexible approach. *J Ad Hoc Netw* 8(3):328–344
9. Enam RN, Imam M, Qureshi R (2012) Energy consumption in random cluster head selection phase of WSN. *IPCSIT*, vol 30
10. Bezdek JC, Egrlich R, Full W (1984) FCM: the fuzzy c-means clustering algorithm. *Comput Geosci* 10:191–203
11. Hoang DC, Kumar R, Panda SK (2010) Fuzzy C-Means clustering protocol for wireless sensor networks. In: *IEEE international symposium on industrial electronics*, pp 3477–3482
12. Su S, Zhao S (2018) An optimal clustering mechanism based on Fuzzy-C means for wireless sensor networks. *J Sustain Comput: Inf Syst* 18:127–134

13. Singh DP, Bhateja V, Kumar S (2013) An efficient cluster-based routing protocol for WSNs using time series prediction-based data reduction scheme. *IJMTIE* 3(3):18–34
14. Singh DP, Bhateja V, Kumar S (2014) Energy optimization in WSNs employing rolling grey model. In: International conference on Signal Processing and Integrated Networks (SPIN), IEEE
15. Pawan Singh M, Najmud Doja M, Alam B (2020) Fuzzy based enhanced cluster head selection(FEBCS) in WSN. *J King Saud University* 32:390–401
16. Sasikumar P, Khara S (2012) K-Means clustering in wireless sensor networks. In: Fourth international conference on computational intelligence and communication networks, vol 136

Implementation and Performance Analysis of PEGASIS and MIEEPB Protocols in Wireless Sensor Networks



Trupti Shripad Tagare and Rajashree Narendra

Abstract Wireless Sensor Networks (WSNs) are deployed in geographical regions with less accessibility to monitor its physical conditions, and also, the data needs to be transmitted to the sink for further processing and analysis. Sensor nodes form the basic element of a WSN. The primary requirement of WSN is to enhance the lifetime of network. Accordingly, different types of routing protocols are implemented and categorized into flat routing, hierarchical and location-based protocols. Here, we consider the implementation and performance analysis of chain-based protocol: Power Efficient Gathering in Sensor Information Systems (PEGASIS), in which the sink is fixed at a location, and its improved version: Mobile Sink Improved Energy-Efficient PEGASIS-based Routing Protocol (MIEEPB) where the sink is dynamic. MATLAB tool is used for simulation of protocols for various parameters. The analysis proves that MIEEPB is a better technique with mobile sink support when compared to PEGASIS which has a fixed sink location.

Keywords WSN · PEGASIS · MIEEPB · Average energy · Dead nodes · Energy efficiency · Protocols

1 Introduction

A Wireless Sensor Network (WSN) consists of many tiny sensor nodes. These nodes sense the parameters of the surrounding environment and transmit the sensed data to the sink node often called as the base station (BS). The node is equipped with a limited source battery. Hence, the power in these sensor nodes needs to be efficiently utilized to improve the network lifetime [1–4]. Figure 1 represents the framework

T. S. Tagare (✉)

Dayananda Sagar College of Engineering, Bengaluru, India
e-mail: truptitagare-ece@dayanandasagar.edu

R. Narendra

Dayananda Sagar University, Bengaluru, India
e-mail: rajashree-ece@dsu.edu.in

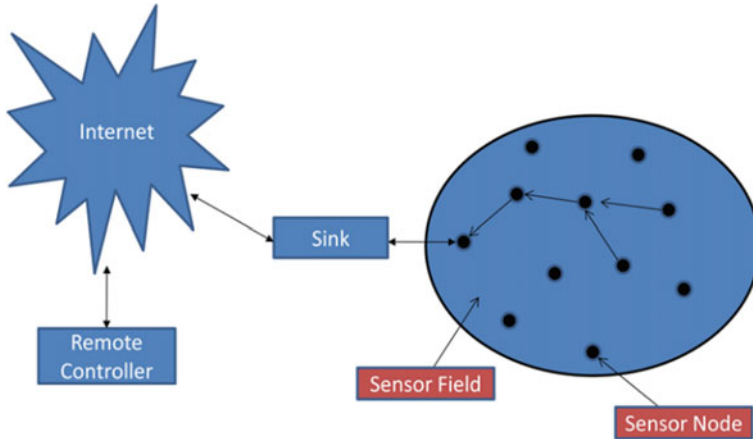


Fig. 1 The framework of WSN [5]

of WSN. Many researchers have proposed numerous routing protocols for efficient consumption of energy and thereby improve the lifetime of WSN.

The techniques are basically categorized as follows:

- **Flat routing-based protocols**—Here, the sensor nodes sense the physical phenomena and either flood or broadcast the data centric characteristics to the base station (BS) [6]. Direct transmission and Minimum Transmission Energy (MTE)-based protocols are few types of protocols
- **Hierarchical-based protocols**—LEACH, LEACH-C (LEACH-Centralized), EAMMH, DEEC, EDEEC and SEP are few **clustering-based hierarchical techniques** which utilize the information like average energy, the separation between the node and base station and remaining energy in each node to select the cluster head. PEGASIS, Hierarchical PEGASIS protocol and MIEEP are a few techniques which use the **chain-based protocol** approach to carry out the communication. [3, 7].
- **Location-based protocols**—These require the ordinates of the node to track the node location for communication purposes. Global Positioning System (GPS) or Non-GPS-based approaches are the two techniques employed which are applicable for both static and mobile nodes [5, 6].

In this work, we analyse the hierarchical chain-based routing protocols, the PEGASIS and MIEEPB. PEGASIS follows a greedy algorithm. The two steps used in the implementation of PEGASIS are chain formation and data gathering. Here, very long chain of nodes is formed [8]. MIEEPB has a mobile sink. It builds smaller chains and thereby reduces the load on the cluster head. The mobility of the sink further helps in reducing the energy consumption for all the nodes. The multi-chain concept helps to reduce distance between nodes [6]. Thus, in this study, we carry

out the performance analysis of PEGASIS and MIEEPB protocols using MATLAB 2020a.

2 Previous Works

- Paper [1] elaborated on the need of energy efficiency in WSN and implemented direct communication, LEACH, energy and distance-based algorithms for few nodes and concluded that LEACH outperformed the other techniques. The work was carried out on MATLAB and Simulink and developed a GUI to represent the energy spent by the nodes in implementation of all the basic algorithms.
- In [8], the authors addressed long distance problem between the nodes and base station in the unique PEGASIS. They proposed an improved PEGASIS protocol which provided better energy efficiency and lifetime when compared with unique PEGASIS.
- [9] gave an insight of different chain-based protocols available and provided the survey details for the following types PEGASIS-ANT, H-PEGASIS, PDCH and IEEPB. It compared the lifetime and energy consumption in these protocols.
- While in [6], the author provided a detailed insight of the hierarchical protocols and carried out a comparative study between MODLEACH and MIEEPB routing protocols with results showing better performance of MIEEPB over MODLEACH. It was implemented using MATLAB and showed the comparison of dead nodes and residual energy left in nodes for MODLEACH and MIEEPB.
- In [5], the location-based clustering approaches extensively detailed on the network architecture, normal sensor node working and energy consumption and classification of location-based routing algorithms. It also implemented the different types, namely GPS and Non-GPS based.
- [10] implemented the enhanced PEGASIS with a mobile sink and to overcome the hot spot problem by determining the communication distance and adjusting the range of nodes and mobile sink according to a set energy threshold. The simulations showed that enhanced PEGASIS showed significant improvement in network lifetime and reduced latency.

3 Objective

For WSN, protocols with high energy efficiency are required to increase the network lifetime. Here, we implement and perform comparative analysis of only the chain-based protocols, namely Power Efficient Gathering in Sensor Information Systems (PEGASIS) and Mobile Sink Improved Energy-Efficient PEGASIS-based Routing Protocol (MIEEPB). The different cases are considered for the study with variation in number of nodes and transmissions.

4 Chain-Based Protocols

4.1 Power Efficient Gathering in Sensor Information Systems (PEGASIS) Protocol

Here, all the sensor nodes transmit the sensed data to its nearest neighbour and in turn create a chain like connection that is established between all the nodes. Finally, the node nearest to BS transmits the data. Figure 2 represents the topology of PEGASIS protocol.

Assumptions

- The BS is situated at a far-off distance from the sensing area.
- Nodes are static in nature.
- Nodes are with same initial energy of 2 J

Simulation Parameters set

Table 1 contains the simulation parameters considered.

Simulation Details

Figure 3 represents the random distribution of chain-based homogeneous nodes in network field area of $100\text{ m} \times 100\text{ m}$ (Fig. 4).

The simulations are executed for the following cases:

CASE 1: Number of operational nodes per transmission (with varied number of nodes).

Fig. 2 Topology of PEGASIS protocol

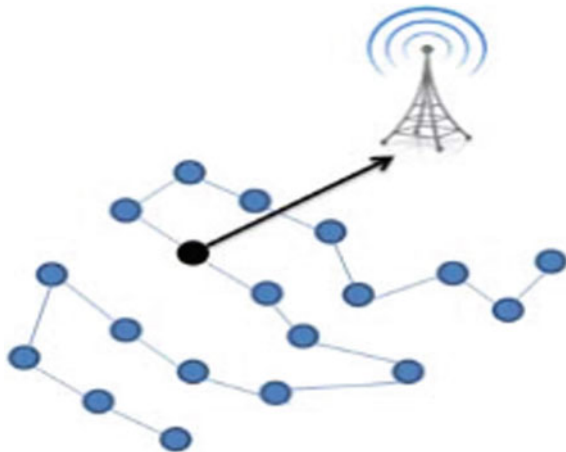


Table 1 Simulation parameters for PEGASIS

Simulation parameters	Values
Network area	100 m × 100 m
Number of nodes (varied)	100, 200
Fixed sink location	50,200
Initial energy: E0	2 J
Eelec = Etx = Erx	50 nJ
Energy spent in the amplifier	100 pJ
Size of data package	4000 bits

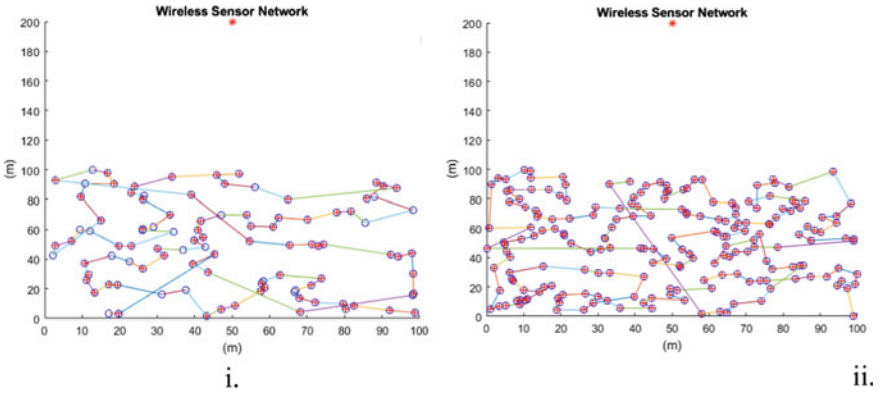


Fig. 3 The random distribution of chain-based homogeneous nodes in a network field: 100 m × 100 m with i. Nodes = 100 ii. Nodes = 200

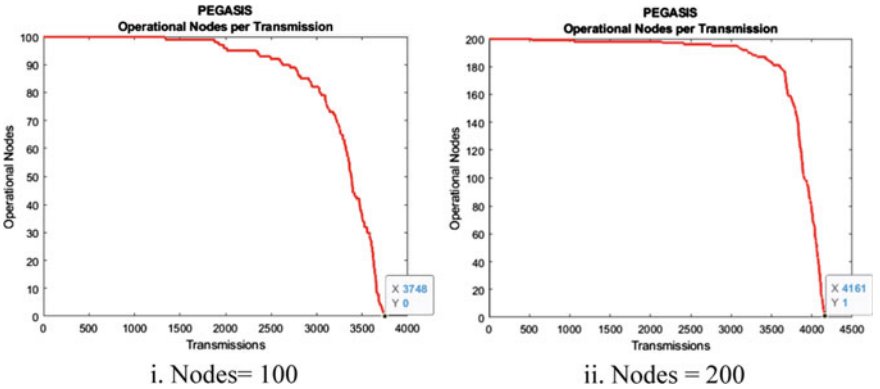


Fig. 4 PEGASIS protocol: number of operational nodes per transmission

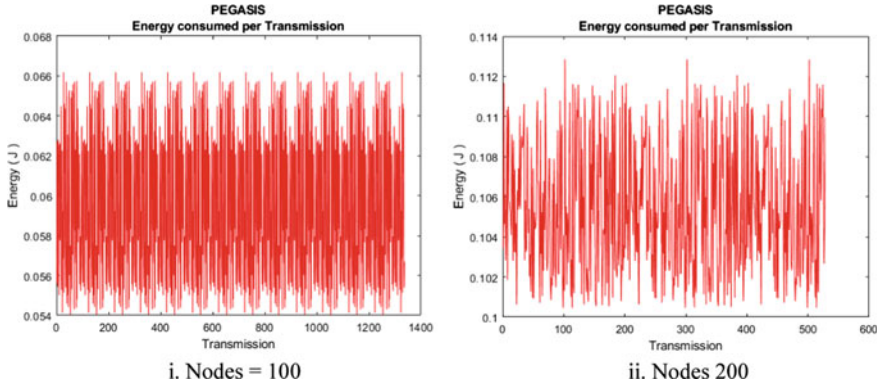


Fig. 5 PEGASIS protocol: energy consumed per transmission with i. Nodes = 100 ii. Nodes = 200

Observation:

The results show that the number of operational nodes per round decreases when the number of nodes in the network is increased from 100 to 200.

CASE 2: Energy consumed per transmission (with different number of nodes) (Fig. 5).

Observation:

The energy consumed in the network increases significantly with the number of nodes increased from 100 to 200. When there are 100 nodes, the energy consumed per transmission goes maximum to 0.66 J on an average; however, with 200 nodes, the energy consumed per transmission increases to 0.113 J.

Advantages of PEGASIS

- For most nodes, the transmitting distance reduces.
- Each node gets selected as the leader, so energy dissipation is balanced among the nodes.

Disadvantages of PEGASIS

- When head node is selected, only its distance from the BS is calculated and not its residual energy.
- Only one leader is selected per transmission which can cause huge congestion and thereby delay in the network.
- Lot of redundant data is transmitted.

Table 2 Simulation parameters for: MIEEPB

Simulation parameters	Values
Network area	100 m × 100 m
Number of nodes (varied)	200
Initial energy: E0	0.5 J
Eelec = Etx = Erx	50 nJ
Energy spent in amplifier types: Efs Emp	10 pJ 0.013 pJ
Energy required in Data Aggregation: EDA	5nJ
Size of data package	4000 bits
Number of data transmissions (varied)	1000, 5000

4.2 Mobile Sink Improved Energy-Efficient PEGASIS-Based Routing Protocol (MIEEPB)

Here, the BS is dynamic. The MIEEPB protocol is an enhanced version of PEGASIS which utilizes the energy more efficiently when compared with PEGASIS protocol. It operates with lesser delay as it divides the total field into small sectors and creates a chain within these sectors. This reduces the length of the chain and suitably utilizes the advantages of PEGASIS protocol. It reduces the distance between attached chains.

Assumptions

- The BS is mobile in nature.
- Homogeneous nodes with same initial energy of 0.5 J

Simulation Parameters

Table 2 shows the simulation parameters considered.

Simulation Details

The chain-based MIEEPB is simulated using MATLAB 2020a.

The simulations are executed for the following cases:

CASE 1: The residual energy per round is varied with respect to number of data transmissions. Figure 6 represents the residual energy per round.

Observation:

The residual energy remains per round with increase in the number of data transmissions.

CASE 2: The normalized average energy per round is varied with respect to number of data transmissions which is represented in Fig. 7.

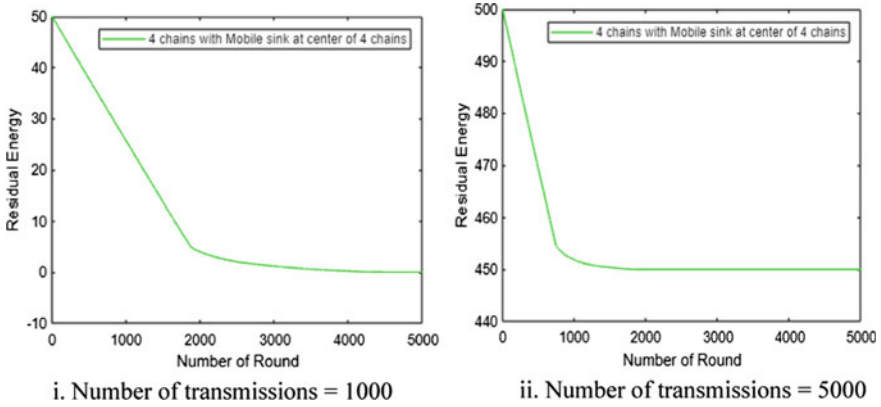


Fig. 6 The residual energy per round (J)

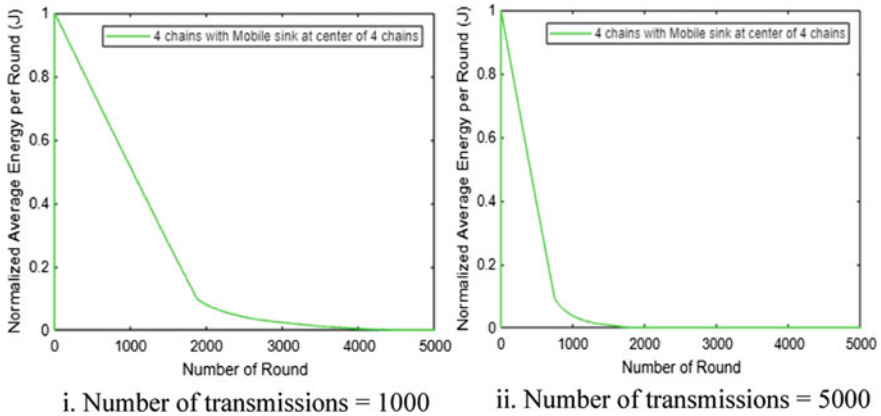


Fig. 7 The normalized average energy per round (J)

Observation:

The normalized average energy remains reduced per round with increase in the number of data transmissions.

CASE 3: The number of alive nodes per round is varied with respect to number of data transmissions as shown in Fig. 8.

Observation:

The number of alive nodes reduces per round with increase in data transmissions from 1000 to 5000 bits.

CASE 4: The number of dead nodes per round is varied with respect to number of data transmissions. Figure 9 represents the number of dead nodes per round.

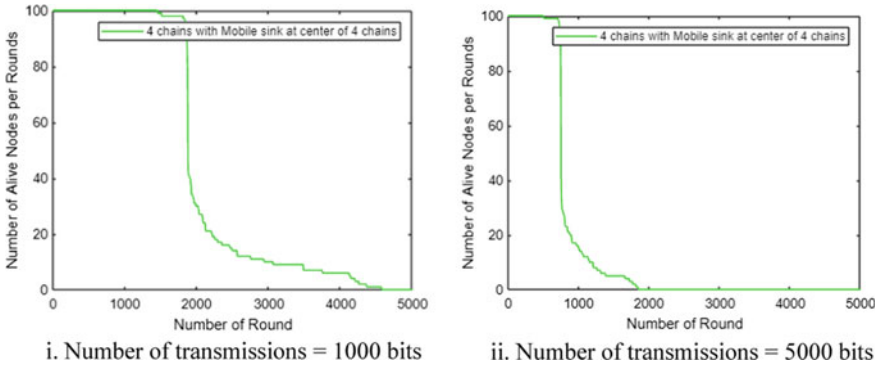


Fig. 8 The normalized average energy per round (J)

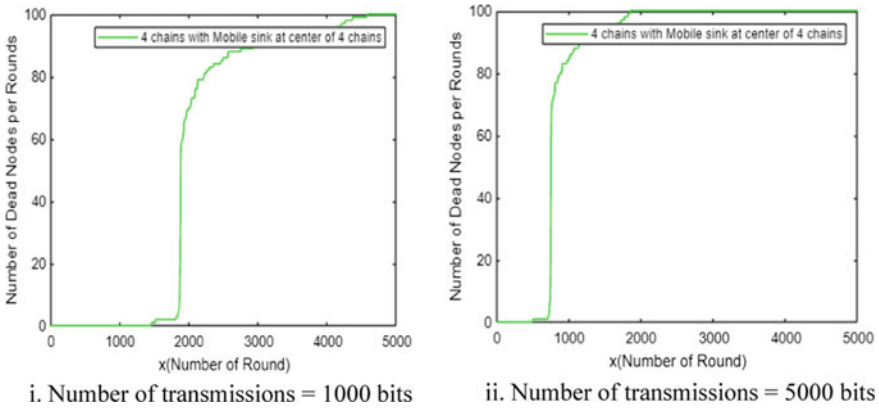


Fig. 9 The dead nodes per round (J)

Observation:

As seen in Fig. 9, for MIEEPB protocol, the number of dead nodes increases per round with increase in the number of data transmissions.

Thus, MIEEPB protocol overcomes the shortcomings of PEGASIS protocol. The MIEEPB takes into account both the distance and residual energy in selection of a leader. This protocol can be applied to forest fire detection scenario where the nodes are statically placed in the forest region and the mobile sink can be a handheld PDA which is with the firefighting service agent.

5 Conclusion

Most of the WSN applications need longer network lifetime. To achieve this, we presented the chain-based protocols in this paper, namely PEGASIS and MIEEPB protocol. Such comparison has not been attempted earlier as per the literature survey done. The simulation results show that PEGASIS protocol is less effective when the long chain of sensor nodes is formed. More energy is consumed to transmit data over the long chain and introduces lot of delay. However, the MIEEPB protocol forms sectors in the network and accordingly forms smaller chains and hence uses the energy efficiently. Thus, it can be concluded that MIEEPB is a better technique with mobile sink support when compared to PEGASIS which has a fixed sink location.

References

1. Tagare TS, Narendra R, Manjunath TC (2021) A GUI to analyze the energy consumption in case of static and dynamic nodes in WSN. In: Shakya S, Bestak R, Palanisamy R, Kamel KA (eds) Mobile computing and sustainable informatics. Lecture Notes on Data Engineering and Communications Technologies, vol 68. Springer, Singapore. https://doi.org/10.1007/978-981-16-1866-6_40
2. Lindsey S, Raghavendra CS (2002) PEGASIS: power-efficient gathering in sensor information systems. In: Proceedings, IEEE aerospace conference, 2002, pp. 3-3. <https://doi.org/10.1109/AERO.2002.1035242>
3. El Ouadi RE, Hasbi A (2020) Comparison of LEACH and PEGASIS hierarchical routing protocols in WSN. In: iJOE, vol 16, no 9. <https://doi.org/10.3991/ijoe.v16i09.14691>
4. Tagare TS, Narendra R (2021) Comparison of clustering techniques for reduction in energy consumption in wireless sensor networks. In: Conference proceedings of NCRTE-2021, published in Shodhsamhita: Journal of Fundamental & Comparative Research, vol VII, no. 3. ISSN 2277-7067
5. Kumar A, Shwe HY et al (2017) Location-based routing protocols for wireless sensor networks: a survey, published by Wireless Sensor Network, vol 9, no 1, 2. <https://doi.org/10.4236/wsn.2017.91003>
6. Zayed H, Taha M, Allam AH (2018) Performance evaluation of MODLEACH and MIEEPB routing protocols in WSN. In: 2018 international conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC); with catalog No. efp18037-PRJ: 978-1-5386-430-7, during 28–29 January 2018 at Priyadarshini Engineering College, Vaniyambadi, India
7. Raza M, Javaid N, Javaid A, Khan ZA (2013) Maximizing the lifetime of multi-chain PEGASIS using sink mobility. World Appl Sci J 21(9):1283–1289 (ISI-Indexed)
8. Kumar VK, Khunteta A (2018) Energy efficient PEGASIS routing protocol for wireless sensor networks. In: 2nd International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), pp 91–95. <https://doi.org/10.1109/ICMETE.2018.00031>
9. Rana H, Vhatkar S, Atique M (2014) Comparative study of PEGASIS protocols in wireless sensor network. IOSR J Comput Eng (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, vol 16, issue 5, Ver. I (Sep–Oct 2014), pp 25–30
10. Wang J, Gao Y, Yin X et al (2018) An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks. In: Wireless communications and mobile computing. Article ID 9472075. <https://doi.org/10.1155/2018/9472075>

A Queue Management System for Cloud Data Processing



Arif Ahmad Shehloo and Muheet Ahmed Butt

Abstract With cloud computing, businesses have to manage their systems effectively due to the amount of data they store every day. The Hadoop Distributed File System with MapReduce is an efficient and widely used cloud data processing platform that parallelizes data processing operations. However, Hadoop's efficiency is heavily reliant on job scheduling. Centralized schedulers offer predictable execution at the cost of resource utilization; distributed schedulers, on the other hand, maximize cluster utilization but have lengthy job completion times when assignments are heterogeneous. The introduction of queues at operational nodes may help to resolve this issue. This paper introduces a queue management system to reduce job execution time while utilizing the system resources as effectively as possible. To achieve rapid job completion times, we can define policies that can be used to manage active queues, in which we specify which task will be executed next when a running task terminates. The proposed system's performance is evaluated using three parameters: total time, average time, and capacity utilized.

Keywords Big data · MapReduce · Hadoop · HDFS · Scheduling

1 Introduction

The term "Big Data" refers to the collection of massive datasets (both structured and unstructured), which is highly challenging to store and process using conventional database systems and software. As a result of the difficulty of analyzing large distributed datasets, Web search companies coined the term "Big data" [1]. Big data is

A. A. Shehloo (✉)

Research Scholar, Mewar University, Chittorgarh, Rajasthan, India

e-mail: arif4aziz@gmail.com

M. A. Butt

P.G Department of Computer Science, University of Kashmir, Srinagar, Jammu and Kashmir, India

e-mail: ermuheet@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023

55

S. C. Satapathy et al. (eds.), *Computer Communication, Networking and IoT*,

Lecture Notes in Networks and Systems 459,

https://doi.org/10.1007/978-981-19-1976-3_6

an emerging technology that will dominate the world in the not-too-distant future. Both technical and marketing information is concealed under this buzzword [2].

Big data processing is made possible by Apache Hadoop, a freely available Java-based programming platform that allows for processing massive quantities of data in a petabyte-scale range in a distributed computation environment [3]. Apache Lucene designer Doug Cutting initially created Hadoop as an essential component of his Web search engine Apache Nutch. Hadoop is an open-source framework for distributed computing that uses the Google MapReduce framework as well as Hadoop Distributed File System (HDFS) [4].

Apache Hadoop is a well-known open-source data storage and processing framework that uses low cost and readily available hardware components to build its clusters. The key to Hadoop's low I/O cost is that the computation process is passed to the data rather than the data being passed to the computation process. A Hadoop framework typically includes two main components: a distributed storage module called Hadoop distributed file system (HDFS) and a distributed processing module called Hadoop MapReduce (supported by YARN in Hadoop 2. x) [3]. Hadoop was designed to run on large networked clusters with master node (responsible for running the services that control Hadoop's storage and processing component) and slave nodes (responsible for storing and processing distributed data). Each slave node contains a daemon (a background process) called the DataNode, which monitors and updates the state of the data regularly to the master node daemon, called the NameNode. When a file is forwarded to HDFS, it is divided into equal-sized data blocks, and three replicas of each are maintained across the Hadoop cluster. That is, a large number of data blocks need to be tracked down. To address this, NameNode uses an information catalog that validates the blocks that comprise the files and tracks down these blocks and their replicas. Without a doubt, storing this type of information elevates the NameNode to a compulsory module in a Hadoop cluster. If a Hadoop cluster's NameNode becomes unreachable, the data stored in HDFS becomes inaccessible to the tasks running on the cluster. In order to minimize the impact on the overall system, a secondary NameNode is used to take checkpoints on the file system metadata stored on the primary NameNode. It simply checkpoints the file system namespace of the namenode but cannot replace the primary Namenode [5].

Despite the massive amounts of data that Hadoop processes, most of its jobs attempt to run indefinitely. If the jobs fail after a long period of time, it is a huge setback. Therefore, jobs must be scheduled appropriately to avoid this, and the user must have some control over the scheduling process. Even though numerous job scheduling techniques have been developed, most of them focus on fairness and resource utilization, with little attention to the time it takes to complete a job. This paper implements a queue management system to optimize the use of system resources and reduce job completion times.

2 Related Work

Big data has signaled the dawn of the terabyte era, in which massive amounts of data are produced at a rapid pace. As the storage capacity, processing power, and data availability rise, global data volume grows in zettabytes. Hadoop is a big data solution that uses the Hadoop Distributed File System and MapReduce to store and analyze the data. To achieve high performance in the Hadoop cluster, it is essential to schedule jobs efficiently to manage the resources. Scheduling in Hadoop provides the ability to process and complete many jobs within a short amount of time. However, numerous job scheduling algorithms consider problems of fairness, data locality, energy efficiency, and resource awareness but do not give much consideration to the job's execution time [8].

Among the multiple schedulers available, the defaults FIFO, capacity, and fair schedulers are well-known. Hadoop's default scheduler operates with a FIFO queue, which means jobs are executed in order of arrival. Nevertheless, this does not ensure that resources are distributed fairly among users. On the other hand, a fair scheduler seeks to allocate cluster capacity and system resources equitably. As a result, it provides significantly better resource utilization, as well as support for preemption. In a multi-tenant cluster environment, the capacity scheduler by Yahoo is specifically designed to run Hadoop applications for maximum throughput and utilization of the cluster. Multiple queues are constructed in capacity scheduling, each containing a configurable number of map and reduce slots. Each queue is guaranteed to have a certain capacity. Queues are constantly monitored to make sure they do not exceed their designated capacity. Any remaining capacity of a queue can be temporarily assigned to other queues if it is not consumed in the allotted time. With capacity scheduling, higher-priority tasks are received resources earlier than tasks with lower priorities. Queues are subject to rigorous access controls in capacity scheduling, limiting the ability to submit jobs to queues and view and modify jobs in queues [7–9].

Job scheduling is primarily influenced by data locality, synchronization, and fair resource allocation. He et al. [10], Xie et al. [11] emphasize the importance of increasing the data locality rate. A matchmaking system was introduced to improve the localization of data for map tasks. In order for each node to have the same chance of claiming its local tasks, the locality marker is used [11]. The job-aware scheduling strategy discussed in [12] can reduce the overall average wait time in heterogeneous clusters, but it could be reduced further.

The most significant benefits of using Hadoop MapReduce are that the data are spread optimally within the HDFS and that the tasks are performed over locally stored data whenever possible, as opposed to other approaches [4, 5]. As a result, data migration among cluster nodes is minimized, and the cluster's performance is improved. In order for Hadoop to perform efficiently with big data, the data must exist in the HDFS. The vast majority of real-world instances, on the other hand, involve data that are produced by existing systems and technologies and then pushed into HDFS for analysis.

In order to complete MapReduce jobs on time, worker nodes must respond immediately. However, current scheduling methods do not provide timely responses to meet the given deadline. With the result, Hadoop's response time and the time required to complete various MapReduce jobs continue to increase. To address this issue, several studies, including [13–15] and [16], have demonstrated how to optimize the map/reduce task completion time by coordinating tasks growth with scheduling and allocating resources. However, all these strategies suffer from limitations, including network bottlenecks, delay in response time, and start-up/step-down costs for map/reduce tasks.

Other studies optimizing Hadoop's effectiveness following the time constraint includes [16–18], and [19]. These scheduling strategies define the tasks that must be completed within a specified time frame while also verifying the availability of resources required to complete those tasks. The job is scheduled only if the specified number of resource slots are available. However, these strategies are predicated on certain assumptions, including the absence of node failures before and following job scheduling, and thus suffer from various limitations.

Hadoop's performance suffers in heterogeneous environments. Therefore, significant research has been conducted, including [20] a block rearrangement algorithm called Saksham for optimizing processing time in a heterogeneous environment via efficient Hadoop file system management. The proposed scheme effectively optimizes significant data processing in both homogeneous and heterogeneous environments.

It is challenging to plan for the growing number of functions and resources robustly. Furthermore, the problem is exacerbated by the possible heterogeneity in Hadoop clusters. Seethalakshmi and Govindasamy [21] proposed a scheduler that makes scheduling decisions to resolve this issue. The test results show that the proposed scheduler outperforms existing systems in terms of overall performance and reliability.

There has been a recent development of job scheduling methodologies, as indicated by the literature [10–21]. However, no significant advances have been made to reduce the time it takes to accomplish a task. Depending on how long it takes a job to execute, the workload on the cluster will be reduced, and resources will be used more efficiently. Thus, we proposed a queue management system in this paper that schedules jobs using a pipelining approach to minimize the time to complete them while optimizing resource utilization.

3 Proposed Work

A NameNode and a DataNode are required to form the proposed system, with the NameNode as the master node and the DataNode being the worker node. Using the NameNode to monitor the DataNode, storing all the metadata required to monitor it, and keeping the DataNode to keep the actual data, will significantly simplify the process. A job is composed of numerous subtasks, either the map or reduce task.

Additionally, the system uses Yahoo’s Capacity Scheduler (which incorporates hierarchical queues, guaranteed capacity, and accessibility) to minimize job execution time while maximizing system resource usage. This work is focused on improving the management of local queues within nodes.

To construct our queue management system that prioritizes job execution time, we have two steps: (1) introducing queues with variable capacity at worker nodes Alpha, Beta, and Default, as discussed in Algorithm 1; and (2) identifying the node to which each task is queued, as discussed in Algorithm 2.

1. In `capacity-scheduler.xml`, the parameter `yarn.scheduler.capacity.*queue-path.capacity` must be edited to set the percentage of cluster resources allocated. In this step, the queues are set to use 50, 30, and 20% of the cluster resources that were previously set by “`yarn.nodemanager.resource.memory-mb`” per `nodemanager`.
2. When a job contains a set of tasks, the scheduler must determine the nodes to which those tasks will be assigned. Now, we present the algorithm for assigning tasks to nodes.

Algorithm 1: Setting up queue capacity

- Step 1: The initial step is to create two new queues (Alpha and Beta).
 - Step 2: Setting up queue capacities.
 - Alpha: capacity is set to 50% of the overall capacity.
 - Beta: capacity is set to 30% of the overall capacity.
 - Step 3: Set up the system’s default queue. Default: capacity is set to 20% of the total capacity.
 - Step 4: Setting up the queue’s access control, status, and resources.
 - Step 5: Restart the Resource Manager for the configuration to take effect after saving the configuration.
-

Algorithm 2: Task Placement

- Step 1: The algorithm takes a task as input and outputs the node that should host the task.
 - Step 2: Jobs are distributed among nodes with available resources (memory and CPU), reducing queue delays. As a result, we determine whether such resources exist first, and if they do, we assign the task to a node with available local resources based on other factors such as data locality.
 - Step 3: Determine which node’s queue to place the task in if the cluster is nearly full.
 - Step 4: The score function determines a node’s suitability for task execution. The score of a node is determined by two factors: task affinity and node load. We currently consider only data locality; this may be extended to incorporate resource interference to provide greater resource isolation when tasks are executed. Using queue capacity and queue wait time, we can calculate the node’s load. Resource Manager measures queue wait time by assuming that each node broadcasts information about the estimated amount of time a task will need to wait at a node before execution begins.
-

4 Results and Discussion

Test analyses were carried out using Hadoop 2.7.3, Ubuntu 12.04, CPU (4Core) N3530@2.16GHz, 4GB RAM and three Test Bed Applications WordCount, Word-mean, and Multiple File WordCount, as shown in Table 2. The performance of the

Table 1 Evaluation parameters

Parameter	Detailed description
Total time	The term “total time” denotes how much time is needed to complete a job in its entirety. Expressed in seconds, it represents the total time spent on the map and reduce tasks
Average MapTime	The “average map time” is calculated as the sum of the timeliness of all map tasks divided by the number of maps executed in the job and can be expressed in seconds
Total capacity utilized	The “total capacity utilized” refers to a parameter that indicates how much capacity a particular task consumes. In addition, it shows how much of the queue’s capacity is being utilized to carry out the task

Table 2 Test Bed applications used

Benchmark application	Detailed description
Wordmean	This program determines the average word length in an input file using MapReduce. A keyword wordmean is used to invoke the program
Wordcount	This program counts the total number of words contained in an input file. A keyword wordcount is used to invoke the program
Multiple file wordcount	This program counts the total number of words in a collection of files. It is a modified version of the program wordcount. It is invoked using the keyword multifilewc

Table 3 Alpha queue efficiency

Benchmark application	Total time (s)	Average MapTime (s)	Average ReduceTime (s)	Average CPUTime (s)	Capacity utilized (%)
Wordmean	57.0	32.0	1.0	3.12	37.5
Wordcount	56.0	31.0	2.0	3.69	25.0
Multiple file Wordcount	51.0	21.0	4.0	3.74	25.0

Table 4 Beta queue efficiency

Benchmark application	Total time (s)	Average MapTime (s)	Average ReduceTime (s)	Average CPUTime (s)	Capacity utilized (%)
Wordmean	52.0	27.0	2.0	3.33	62.5
Wordcount	43.0	16.0	1.0	3.55	41.7
Multiple file wordcount	42.0	14.0	4.0	3.58	62.5

Table 5 Default queue efficiency

Benchmark application	Total time (s)	Average MapTime (s)	Average ReduceTime (s)	Average CPUTime (s)	Capacity utilized (%)
Wordmean	51.0	24.0	1.0	3.23	93.8
Wordcount	44.0	17.0	1.0	3.54	93.8
Multiple file Wordcount	44.0	16.0	2.0	3.77	62.5

Table 6 Queue efficiency for wordmean application

Queue	Total time (s)	Average MapTime (s)	Average ReduceTime (s)	Average CPUTime (s)	Capacity utilized (%)
Alpha	57.0	32.0	1.0	3.12	37.5
Beta	52.0	27.0	2.0	3.33	62.5
Default	51.0	24.0	1.0	3.23	93.8

Table 7 Queue efficiency for wordcount application

Queue	Total time (s)	Average MapTime (s)	Average ReduceTime (s)	Average CPUTime (s)	Capacity utilized (%)
Alpha	56.0	31.0	2.0	3.69	25.0
Beta	43.0	16.0	1.0	3.55	41.7
Default	44.0	17.0	1.0	3.54	93.8

Table 8 Queue efficiency for multiple file wordcount

Queue	Total time (s)	Average MapTime (s)	Average ReduceTime (s)	Average CPUTime (s)	Capacity utilized (%)
Alpha	51.0	21.0	4.0	3.74	25.0
Beta	42.0	14.0	3.0	3.58	62.5
Default	44.0	16.0	2.0	3.77	62.5

proposed queue management system is measured by employing three parameters: the total time, the average map time, and the total capacity utilized, as shown in Table 1. Based on different queue capacities, jobs are assigned to distinct queues, and their execution times are included in Tables 3, 4 and 5. Next, we assess the proposed queue management system's performance based on the total time, average map time, and total capacity utilized, as shown in Tables 6, 7 and 8, respectively. Figures 1, 3, and 5 show the performance graphs for alpha, beta, and default queues, based on total

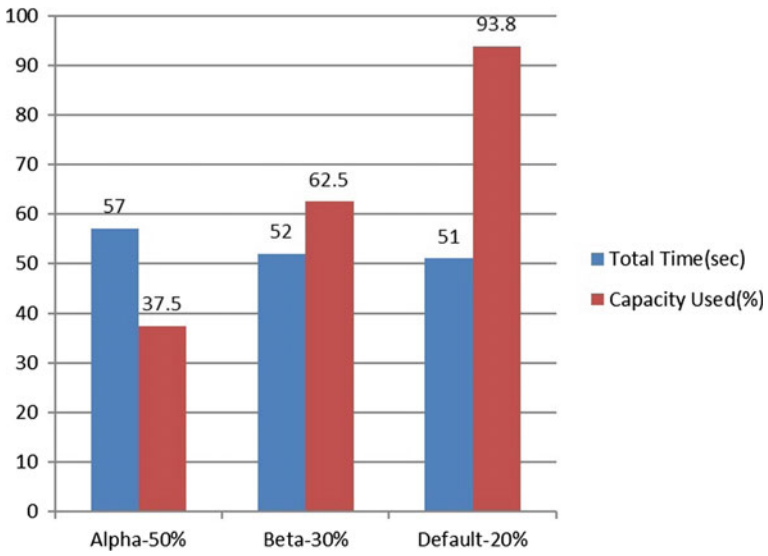


Fig. 1 Wordmean application: total time and total capacity utilized

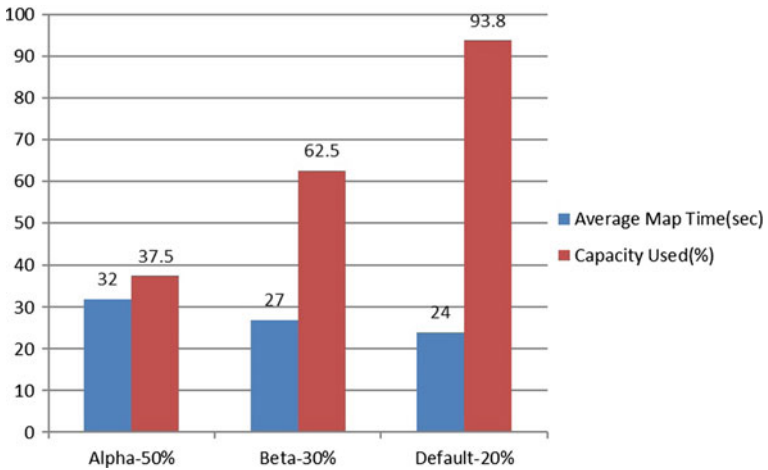


Fig. 2 Wordmean application: average map time and total capacity utilized

time and capacity utilized. Further, Figs. 2, 4, and 6 show the alpha, beta, and default queue performance based on average map time and total capacity utilized. It can be concluded from the results that adding queues at worker nodes improved the capacity scheduler’s performance in terms of job completion time and resource usage.

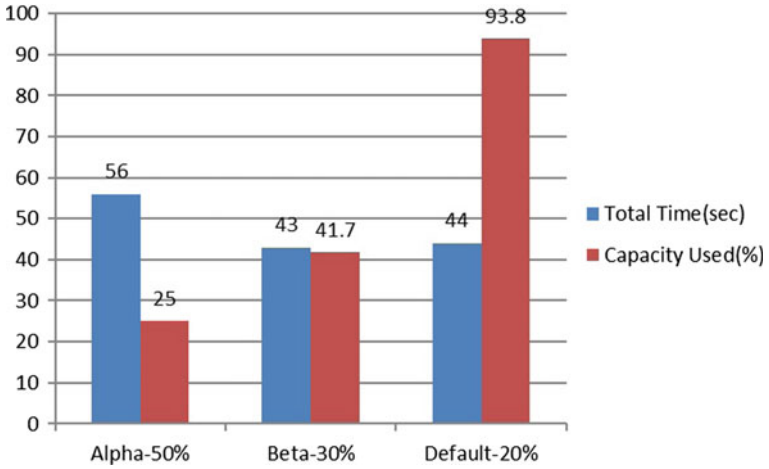


Fig. 3 Wordcount application: total time and total capacity utilized

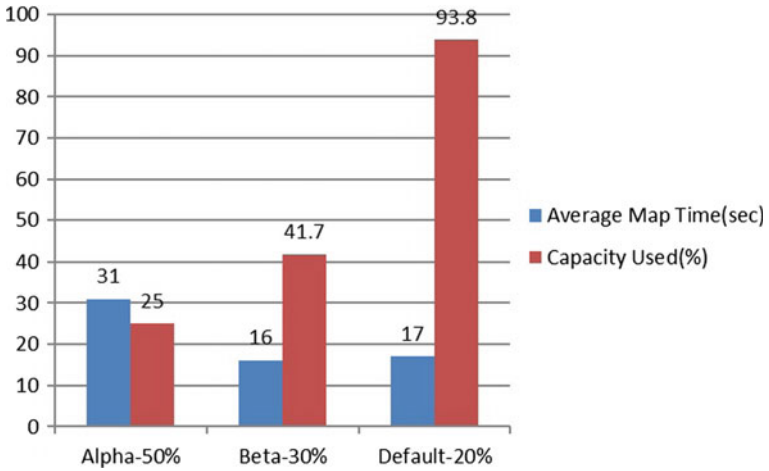


Fig. 4 Wordcount application: average map time and total capacity utilized

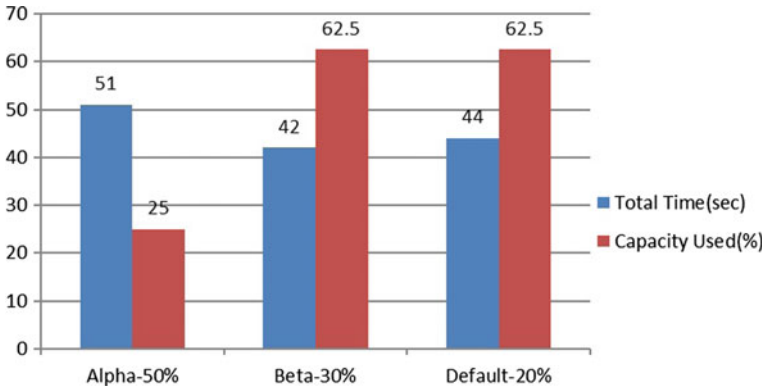


Fig. 5 Multiple File Wordcount application: total time and total capacity utilized

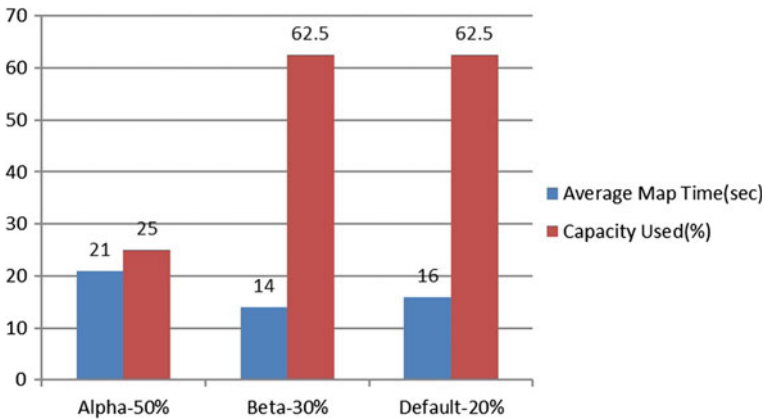


Fig. 6 Multiple File Wordcount application: average map time and total capacity utilized

5 Conclusion

The proposed work aims to decrease the time required to execute jobs and optimize the system’s resource utilization. As part of the cluster infrastructure, the Capacity Scheduler manages resource allocation for multiple concurrent jobs. We can improve a Capacity Scheduler’s execution time and capacity performance with MapReduce benchmark applications by introducing queues with varied capacities at worker nodes. The study’s novel contribution is that by leveraging queues, the use of centralized systems can be comparable to distributed systems. Furthermore, we carefully select which task to complete next when a running task is terminated during active queue management to complete jobs as quickly as possible. Thus, both centralized and distributed scheduling schemes may benefit from our system. This

study analyzes the proposed system's performance using three parameters: total time, average time (for both map and reduce task), and capacity utilized.

Furthermore, when the workload of the cluster is known, the Capacity Scheduler can be employed. Through the capacity scheduler, several users can share Hadoop cluster resources predictably. Furthermore, the capacity scheduler can move unused capacity from infrequently utilized queues to overloaded queues automatically.

6 Future Scope

It is critical to make accurate queue length estimates when working with worker nodes. If queues are sufficiently short, they can result in lower cluster utilization due to idle resources between allocations; if queues are excessively long, they can result in excessive queuing delays. The current work could be expanded to include a multiuser environment to assess scheduling algorithms' performance when confronted with diverse workloads, causing jobs to compete for resources.

References

1. Ashwin Kumar TK, Liu H, Thomas JP, Mylavarapu G (2015) Identifying sensitive data items within hadoop. *IEEE*
2. Saraladevi B, Pazhaniraja N, Victor Paul P, Saleem Basha MS, Dhavachelvan P (2015) Big data and hadoop-a study in security perspective. *Procedia Comput Sci* 50(2015):596–601
3. Apache Hadoop. <http://hadoop.apache.org>
4. Hadoop Distributed file system. http://hadoop.apache.org/docs/r1.0.4/hdfs_design.html
5. Hadoop Distributed file system. http://en.wikipedia.org/wiki/Apache_Hadoop#Hadoop_Distributed_File_System
6. Hamad F (2018) An overview of hadoop scheduler algorithms. *Modern Appl Sci* 12(8):69. <https://doi.org/10.5539/mas>
7. Singh N, Agrawal S (2015) A review of research on MapReduce scheduling algorithms in Hadoop. 2015 International conference on computing, communication and automation (ICCCA). Noida, India, pp 637–642
8. Sreedhar C, Kasiviswanath N, Chenna Reddy P (2015) A survey on big data management and job scheduling. *Int J Comput Appl* (0975–8887) 130(13):41–49
9. Thirumula Rao B, Reddy LSS (2011) Survey on improved scheduling in hadoop MapReduce in cloud environments. *Int J Comput Appl* (0975–8887) 34(9):29–33
10. He C, Lu Y, Swanson D (2011) Matchmaking: a new mapReduce scheduling technique. 2011 IEEE third international conference on cloud computing technology and science (CloudCom). Greece, Athens, pp 40–47
11. Xie J et al (2010) Improving MapReduce performance through data placement in heterogeneous hadoop clusters. 2010 IEEE international symposium on parallel and distributed processing, workshops and Phd forum (IPDPSW). Atlanta, USA, pp 1–9
12. Pati S, Mehta MA (2015) Job aware scheduling in hadoop for heterogeneous cluster. 2015 IEEE International advance computing conference (IACC). Bengaluru, India, pp 778–783
13. Polo J, Castillo C, Carrera D, Becerra Y, Whalley I, Steinder M, Torres J, Ayguad'e E (2011) Resource-aware adaptive scheduling for MapReduce clusters. In: Proceedings of the 12th

- ACM/IFIP/USENIX international conference on Middleware (Middleware'11). Springer-Verlag, Berlin, Heidelberg, pp 187–207
14. Liang Y, Wang Y, Fan M, Zhang C, Zhu Y (2014) Preadoop: preempting reduce task for job execution accelerations 8807:167–180
 15. Pastorelli M, Carra D, Dell' Amico M, Michiardi P (2017) HFSP: bringing size-based scheduling to hadoop. *IEEE Trans Cloud Comput* 5(1):43–56
 16. Verma A, Cherkasova L, Campbell RH (2011) ARIA: automatic resource inference and allocation for MapReduce environments. In: *Proceedings of the 8th ACM international conference on Autonomic computing (ICAC' 11)*. Association for Computing Machinery, New York, NY, USA, pp 235–244
 17. Voicu C, Pop F, Dobre C, Xhafa F (2014) MOMC: multi-objective and multi-constrained scheduling algorithm of many tasks in Hadoop. In: *2014 ninth international conference on P2P, parallel, grid, cloud and internet computing, Guangdong*, pp 89–96
 18. Han J, Yuan Z, Han Y, Peng C, Liu J, Li G (2017) An adaptive scheduling algorithm for heterogeneous Hadoop systems. In: *2017 IEEE/ACIS 16th international conference on computer and information science (ICIS)*, Wuhan, pp 845–850
 19. Cheng D, Zhou X, Xu Y, Liu L, Jiang C (2019) Deadline-aware MapReduce job scheduling with dynamic resource availability. *IEEE Trans Parallel Distrib Syst* 30(4):814–826
 20. Ankit S, Mamta P (2020) Saksham: resource aware block rearrangement algorithm for load balancing in hadoop. *Procedia Comput Sci* 167:47–56
 21. Seethalakshmi V, Govindasamy V, Akila V (2020) Real-coded multi-objective genetic algorithm with effective queuing model for efficient job scheduling in heterogeneous Hadoop environment. *J King Saud Univ Comput Inf Sci*

Sensor Integration and Information Sharing for Automated Electric Vehicles for Better Estimation of the Surroundings



Naarisetti Srinivasa Rao, Reddy Ganesh, K. R. Raghunandan,
D. Radhakrishna, C. Praveenkumar, and Bonthu Kotaiah

Abstract Utilising well-designed energy management strategies, plug-in hybrid electric vehicles (PHEVs) have the potential to be more fuel efficient and emit fewer pollutants on the road than conventional vehicles (EMSs). This vehicle's electronic management system (EMS) has long been a focus of research, and control-oriented approaches like dynamic programming (DP) and model-predictive control have helped achieve optimal or nearly optimal performance. In this work looked into the possibility of encountering model uncertainty, environmental uncertainty and adversarial attacks when using the developed DRL algorithms in real-world applications. A Bayesian ensemble-enabled uncertainty-aware DRL agent was created to address model uncertainty. If the state is unknown, the agent calculates the level of uncertainty associated with the output action. This means that even though actions will be calculated for all input states, the high level of uncertainty associated with unknown or novel states is captured. A risk-aware DRL agent based on distributional RL algorithms was created for environmental uncertainty. Because the decision-making process was based on conditional value at risk rather than expected returns, it gave users more flexibility and could be adapted to suit different application scenarios. Finally, the impact of adversarial attacks on the DRL agents developed using neural networks was evaluated.

N. Srinivasa Rao (✉) · R. Ganesh

Electrical Section, Engineering Department, University of Technology and Applied Sciences-IBRI, Ibri, Al Dhahirah, Sultanate of Oman

e-mail: Naarisetti@ibrict.edu.com

K. R. Raghunandan · D. Radhakrishna

Department of Computer Science and Engineering, N.M.A.M.Institute of Technology, NITTE, Bangalore, India

C. Praveenkumar

Department of Electrical and Electronics Engineering, Sri Ramakrishna Engineering College, Coimbatore, India

B. Kotaiah

Department of CS and IT, Maulana Azad National Urdu Central University, Gachibowli, Hyderabad, Telangana, India

Keywords Electronic management system · Dynamic programming · Dynamic programming · DRL agent

1 Introduction

Due to their zero emissions, low noise, rising oil prices and difficulty in extracting fossil fuels, the demand for electric vehicles (EVs) is growing steadily. The energy management systems (EMSs) in electric vehicles are constantly being improved to cope with their limited driving range, thanks to emerging technologies. An effective energy management system (EMS), like the battery management system (BMS), is required for EMS to function properly and safely. The high-performance battery packs for EV [1] must also be monitored and managed for high reliability and safe operation due to the market's expected rapid growth. The BMS will manage and monitor the EV's EMS battery, as well as many other energy storage functions. An EV battery is made up of a series of batteries, most commonly lithium-ion batteries. A large number of cell elements are found in a high-voltage battery pack, and this creates some difficulties. If one of the cells in a large number of serially connected cells is damaged, it will affect all of the other cells as well. Because EVs operate at high currents and voltages, they must ensure the safety of passengers and other road users. As a result, all of the battery's cells must be regularly inspected to ensure proper operation.

Charge and discharge rates, battery temperature and depth of discharge all affect the battery pack's performance. In order to get the most life out of a battery, it is critical to keep an eye on these battery parameters because they can overheat and explode if overcharged or be destroyed if undercharged. In order to measure the battery's parameters, individual electronic components can be used [2]. However, because there are many cells connected in series and/or parallel, handling and placing these components on a board become tedious. Automotive environments also have extreme temperature variations, dust, wind and water as well as vibrations that can severely damage electronic components.

Hybrid electric vehicles (HEVs) were introduced to reduce inefficient energy use and emissions from transportation fuel combustion. HEVs are now widely used. When braking, HEVs use regenerative technology, which allows the engine to operate within a narrower range whilst using less energy. They can also draw power from the grid to reduce emissions and save money [3]. A minimum of two energy sources are used to power HEVs. Batteries and internal combustion engines are the primary components of most hybrid electric vehicles (HEVs). HEVs that can be recharged from the grid, such as plug-in hybrid electric vehicles (PHEVs), have more powerful electric motors and larger batteries, allowing them to achieve higher fuel efficiency than conventional gasoline-powered vehicles [4]. A good energy management strategy (EMS) is required even though plug-in hybrid electric vehicles (PHEVs) have the potential to achieve high fuel efficiency and low on-road emissions [5].

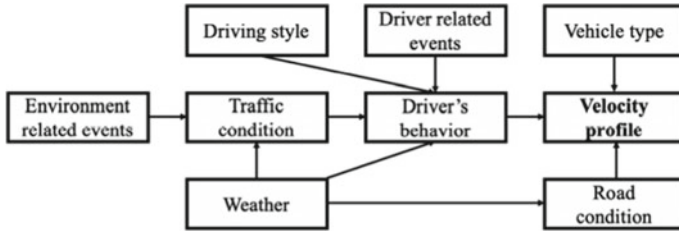


Fig. 1 Generation of real-world velocity profiles

2 Background

Because the velocity profile is determined by so many complex and stochastic factors, it is nearly impossible to know it ahead of time when using OB methods in real-world applications [6]. An example of how velocity profiles are generated in real-world scenarios is shown in Fig. 1. The vehicle’s velocity profile is influenced primarily by two groups of variables: the surrounding environment and the driver. Weather, road conditions, other drivers on the road and special occasions like holidays, sporting events and concerts all factor into the environment. Driving style and the driver’s emotional state are critical factors for the driver.

Due to fluctuating traffic conditions and the fact that road characteristics can be extremely diverse, route has a significant impact on velocity profiles. Because of this, the route is not always predetermined before a trip, as in the case of the delivery vehicle trips analysed in this study [7]. Whilst driving from one place to another, the driver has the option of selecting from a variety of routes depending on their preferences and the current traffic situation. If the order of deliveries can be changed freely or partially, the problem becomes more complex for a package delivery trip [8]. For this reason, predicting future trip information begins with predicting the route. The topic of route prediction is complex because it relies heavily on assumptions.

3 Methodology

The main microcontroller and sub-microcontroller are both found in the control unit. Figure 2 depicts the sub-microcontroller system of interest in this thesis. Battery state estimation and measurement are performed by a sub-microcontroller in this design [9]. Because of this, the firmware can be used to measure and monitor a large number of cells with only a few small changes to the configuration parameters and data storage buffers. Because the company develops the control unit hardware, there was no other option for this this but to use the same hardware. Future versions are expected to use the same control unit hardware. Because the next generation of hardware isn’t yet available, this assumption is made [10]. In terms of memory, ITCM has been set to 32 KB, whilst DTCM has been set to 32 KB.

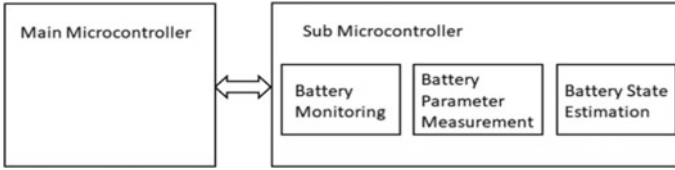


Fig. 2 Architecture for the system

ITCM downloads the entire software image to improve performance. Upon booting, the programme loaded into the ITCM RAM begins running at address $0 \times 00,000,000$. There is an ITCM table for vector data as well [11]. The customised hardware determines how peripheral address space is mapped. HSUART is a type of ultra-rapid serial interface. HSUART 0 and HSUART 1 are two peripherals. The BMS IC can be communicated with using either of these methods [12]. The only HSUART currently in use is HSUART 0. The serial console's output is printed using the UART module. The GPIO module has been included for testing and troubleshooting purposes [13]. SPI 0 is used to measure the current flowing through a device. Bug access ports (DAP), breakpoint units (BPU) and data watchpoints (DWT) are used for debugging in private peripheral bus address space.

4 Implementation and Results

Figure 3 shows the control unit's block diagram, which includes an FPGA implementation module, a chain of BMS ICs, a series of battery cells, a shunt resistance at the end of the chain of cells and an ADC.

The FPGA implements two high-speed UART modules and an integrated ARM Cortex-M1 processor on the microcontroller. The BMS topology explained can be implemented with just one high-speed UART module. A single-BMS IC is connected to a single cell via a BMS bus [13]. The transceiver IC connects the first BMS IC in the chain to the master on one side and the next BMS IC on the other. Master and slave are used to describe the microcontroller and BMS ICs, respectively. The galvanic isolated high-speed UART interfaces on the BMS IC and microcontroller communicate with each other using a proprietary company protocol [14]. The ADC receives the voltage drop measured across the shunt resistance from the differential op-amp, which is connected across it. SPI is used by the microcontroller and ADC to communicate (Fig. 4).

There can be an interpretable white-box post-processing module integrated into the black-box RL system that includes explicit rules for unfamiliar or new states, as shown in Fig. 5, when using an RL algorithm that is aware of uncertainty. It is also possible to regulate the threshold for defining states that are unfamiliar or novel. In this case, the RL-based EMS becomes the widely used interpretable rule-based

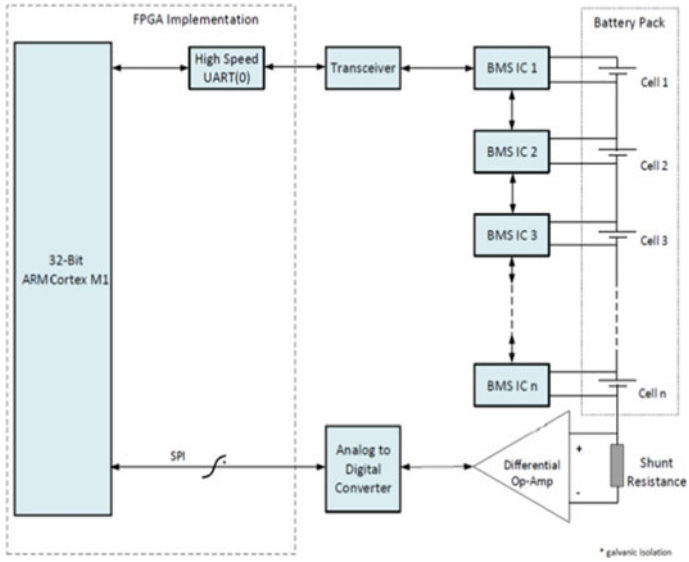


Fig. 3 Control unit block diagram

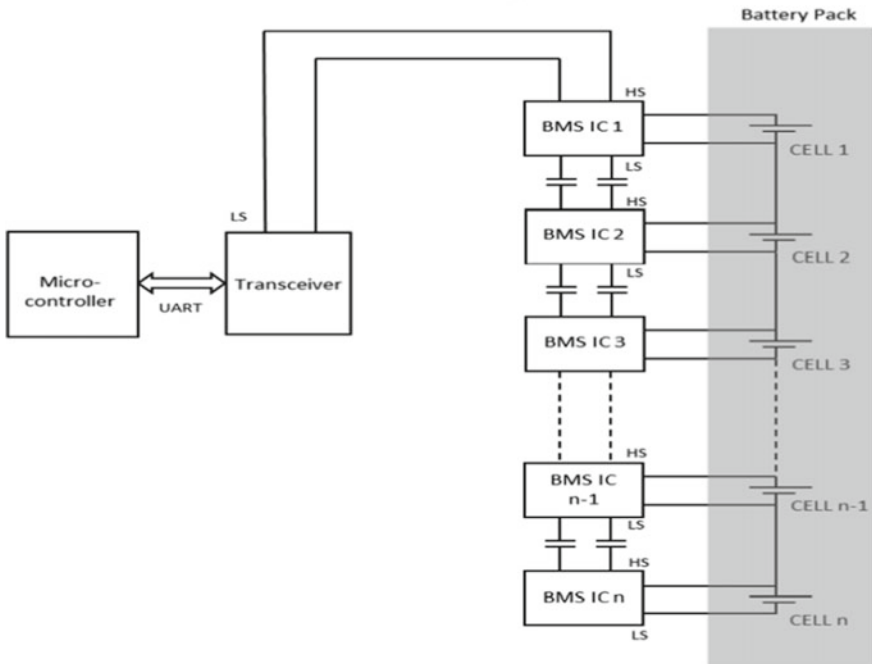


Fig. 4 Master on top (MOT) topology

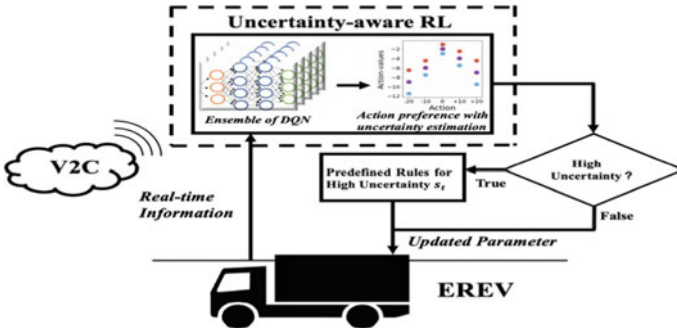


Fig. 5 Framework for the proposed method

EMS when the threshold is set to 0. We can use this example to show how the post-processing module can overwrite the L_{set} with a high value if model uncertainty is greater than some predefined threshold. It can also alert drivers to stop using EREV until the SOC returns to some value. Instead of discussing the design of the post-processing module, this project focuses on creating an RL algorithm that is aware of uncertainty and can identify novel states.

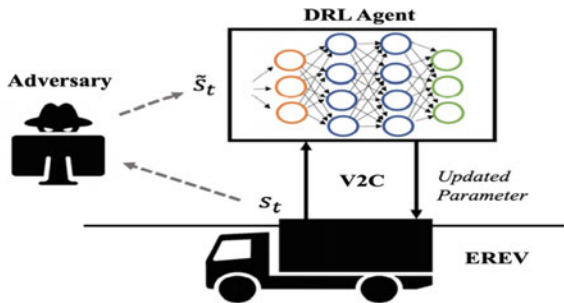
Using FGSM-related methods, I examine the effects of adversarial examples on a well-behaved DRL-based EMS. Methods are classified as either white-box or black-box based on the information that the attacker has access to (Fig. 6).

Adversarial examples on DRL algorithms in ITS are examined in this study, which emphasises robustness and safety. Figure 8 depicts the attack method. There is evidence that adversarial attacks degrade the DRL-based EMS’s performance, resulting in the EREV using too much fuel or running out of battery during the delivery trip, whichever occurs first.

Figure 7 summarises the DQN’s results under FGSM and its two variations. To begin, it is clear that the deep RL-based EMS’s performance is degraded faster when subjected to any of the three versions of noise.

The gradient-based adversarial examples can reduce the agent’s performance by a significant amount for the same magnitude. The adversarial examples, on the other hand, can be much more similar to the original inputs in order to lead the agent to

Fig. 6 Adversarial attack for proposed method



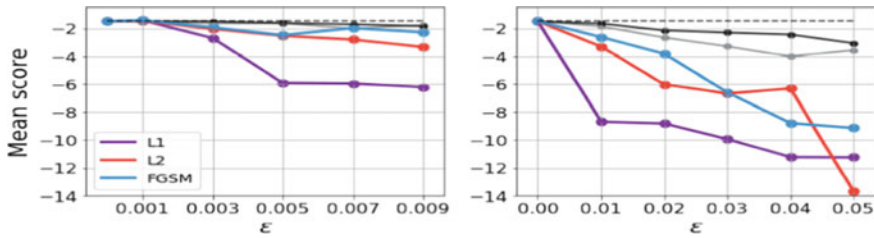


Fig. 7 Performance of the proposed method

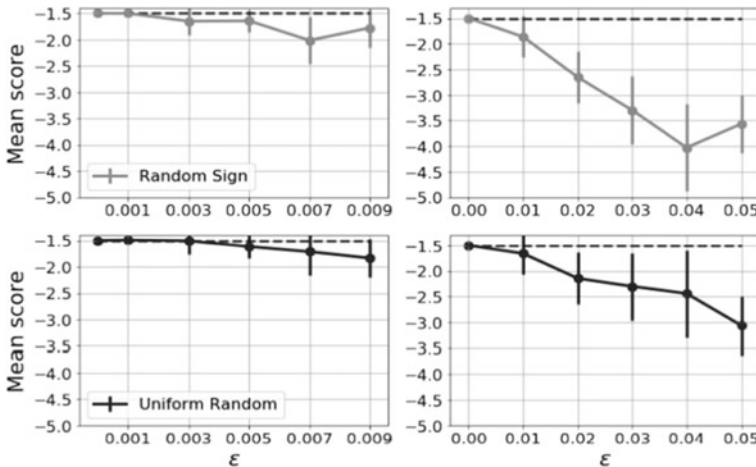


Fig. 8 DQN’s response to two different kinds of noise

perform at a low level. Second, it is clear that the L1-constrained approach is the most effective in the vast majority of situations. In contrast to other methods, however, one major drawback is that it consumes the entire budget to cause an anomaly in a single dimension, making it much easier to detect. This is illustrated in Fig. 8 by the DQN’s response to two different kinds of noise. I conducted ten experiments with a total of ten average results for each value.

5 Conclusion

In the last two decades, energy management system development for HEVs and PHEVs has advanced significantly. It is difficult to predict detailed trip information because of the many complex and stochastic factors in real-world transportation systems. For example, future driving cycles are unknown. Static and dynamic affordance learning was successfully demonstrated in this thesis as an important layer of

perception. In order for self-driving cars to have a comprehensive and universal scene understanding, this layer must be included. Some of the DRL-based methods used in this study are the polar opposite of the Bayesian approach. Using historical delivery trip data to predict future trips is a reasonable assumption. A smart driver-assistant built using historical data and a vehicle model can therefore automatically adjust Lset's value as needed during subsequent trips. To achieve high fuel efficiency, this approach requires careful tuning and validation of each intelligent agent for each vehicle, which may prevent it from being used widely.

References

1. Kalia AV, Fabien BC (2020) On implementing optimal energy management for EREV using distance constrained adaptive real-time dynamic programming. *Electronics* 9(2):228
2. Virtanen P, Gommers R, Oliphant TE, Haberland M, Reddy T, Cournapeau D, Burovski E et al (2020) SciPy 1.0: fundamental algorithms for scientific computing in Python. *Nature Methods* 17(3):261–272
3. Majumdar A, Pavone M (2020) How should a robot assess risk? Towards an axiomatic theory of risk in robotics. In *Robotics Research*. Springer, Cham, pp 75–84
4. Wang P, Northrop W (2020) Reinforcement learning based energy management of multi-mode plug-in hybrid electric vehicles for commuter route. No. 2020-01-1189. SAE Technical Paper, 2020
5. Zhang F, Xiaosong H, Langari R, Cao D (2019) Energy management strategies of connected HEVs and PHEVs: recent progress and outlook. *Prog Energy Combust Sci* 73:235–256
6. Liu K, Li K, Peng Q et al (2019) A brief review on key technologies in the batterymangement system of electric vehicles. *Front Mech Eng* 14:47–64. <https://doi.org/10.1007/s11465-018-0516-8>
7. Giuseppe P, Huo Y, Roeleveld J, Belingardi G et al (2019) Integration of on anselma-line control in optimal design of multimode power-split hybrid electric vehicle powertrains. *IEEE Trans Vehicular Technol* 68(4):3436–3445
8. Stroe N, Oлару S, Colin G, Ben-Cherif K et al (2019) Predictive control framework for HEV: energy management and free-wheeling analysis. *IEEE Trans Intell Veh* 4(2):220–231
9. Rama N, Wang H, Orlando J, Robinette D, Chen B (2019) Route-optimized energy management of connected and automated multi mode plug-in hybrid electric vehicle using dynamic programming. No. 2019-01-1209. SAE Technical Paper
10. Xu B, Malmir F, Rathod D, Filipi Z (2019) Real-time reinforcement learning optimized energy management for a 48V mild hybrid electric vehicle. No. 2019-01-1208. SAE Technical Paper
11. Sun C, Uwabeza Vianney JM, Cao D (2019) Affordance learning in direct perception for autonomous driving. arXiv preprint [arXiv:1903.08746](https://arxiv.org/abs/1903.08746)
12. Xu B, Rathod D, Zhang D, Yebi A, Zhang X, Li X, Filipi Z (2019) Parametric study on reinforcement learning optimized energy management strategy for a hybrid electric vehicle. *Appl Energy* 114200
13. Zhao P, Wang Y, Chang N, Zhu Q, Lin X (2018) A deep reinforcement learning framework for optimizing fuel economy of hybrid electric vehicles. In: 2018 23rd Asia and South Pacific design automation conference (ASP-DAC). IEEE, pp 196–202
14. Hu Y, Li W, Kun X, Zahid T, Qin F, Li C (2018) Energy management strategy for a hybrid electric vehicle based on deep reinforcement learning. *Appl Sci* 8(2):187

Cloud-Computed Solar Tracking System



G. Govinda Rajulu, M. Jamuna Rani, D. Deepa, Udit Mamodiya, Radhika G. Deshmukh, and T. Rajasanthosh Kumar

Abstract Nations in the contemporary world choose renewable energy sources since it is cheaper, cleaner, and more plentiful than fossil fuels. According to recent studies, international airports like CIAL, which operate only on renewable energy, are transforming India into a solar powerhouse. And in the Indian state of Tamil Nadu, one of the giant solar power plants has recently been built. The project's goal is to develop a test device for usage before a solar power plant is created, which will cost a lot of money. Hardware and software are the two components of the project. Arduino, LDR sensors, and servo motors make up the hardware, while a mobile application accesses the graph on the go. Amazon's Web server is used for cloud computing. The LDR sensors provide data to the cloud, where computer operations are carried out. Finally, a graph will be generated as a result of the processing. Using the smartphone app, you may see the chart. We can determine whether the site we are considering for a large project like a solar farm is viable by looking at the graph. With this initiative, we can anticipate the future performance of the solar farm and prepare accordingly.

G. Govinda Rajulu (✉)
CSE Department, St Martins Engineering College, Dhullapally, Secundrabad, Telangana, India
e-mail: rajulug7@gmail.com

M. Jamuna Rani
ECE Department, Sonatech College of Technology Salem, Salem, Tamil Nadu, India
e-mail: jamunarani.m@sonatech.ac.in

D. Deepa
Department of Computer Science and Engineering, Kongu Engineering College, Perundurai, Tamil Nadu, India

U. Mamodiya
Department of Electrical Engineering, Poornima College of Engineering, Jaipur, Rajasthan, India

R. G. Deshmukh
Department of Physics, Shri Shivaji Science College Amravati, Amravati, Andhra Pradesh, India

T. Rajasanthosh Kumar
Department of Mechanical Engineering, Oriental Institute of Science and Technology, Bhopal, India
e-mail: rajasanthosh@oriental.ac.in

As a result, it aids in avoiding significant investments before the project's viability has been determined.

Keywords Cloud computing · Solar tracking system · Data acquisition method · Cloud system

1 Introduction

Solar energy will unquestionably play an essential part in our country's energy destiny [1]. When it comes to environmental effects, the generation and use of green energy are minimal or non-existent. As a result, green energy is becoming more important in developed countries, such as Taiwan, which follows the global trend by pushing its green energy programs. As a result, future generations will rely heavily on renewable energy sources like solar and wind power [2]. As predicted by the authors, a system has been built that takes advantage of the cloud structure to provide an all-encompassing and professional approach to controlling electrical energy. Three critical structural elements are data gathering, storage the data, and application [3].

This platform for managing electric energy will integrate GPS and data collection communication systems, starting with environmental and solar power production monitoring [4]. Temperature, humidity, and light intensity are three of the most critical parameters to monitor when using an ecological monitoring system. The environmental monitoring system, to extract useful information, must include sensors compatible with each other. The solar power monitoring system needs sensors on the inverter to collect data on the output of the solar panels. Ever the preceding subsystems is chock-full of sensors and communication devices [5]. The communication system transfers all sensor data to the relay station, transmitting it to the data storage center across the network. At the central data storage facility, the information for each subsystem is kept in a database as well. Software is required, storage of data to assure collecting speed with the security. Another software technology is used to the data acquired by various pieces of apparatus into helpful needed data by this solar power plant's electric energy management system [6].

2 Monitoring System

2.1 Hardware System

According to Fig. 1, this system's electrical energy measurement gear is built using a three-phase four-wire connection approach. Each phase of the power supply has its transformer for measuring various electric quantities, which is connected to an Arch-meter PA3000 smart meter through a three-phase Y-connector power supply. Each array has a PA3000 installed to keep tabs on the health of the array's solar inverters.

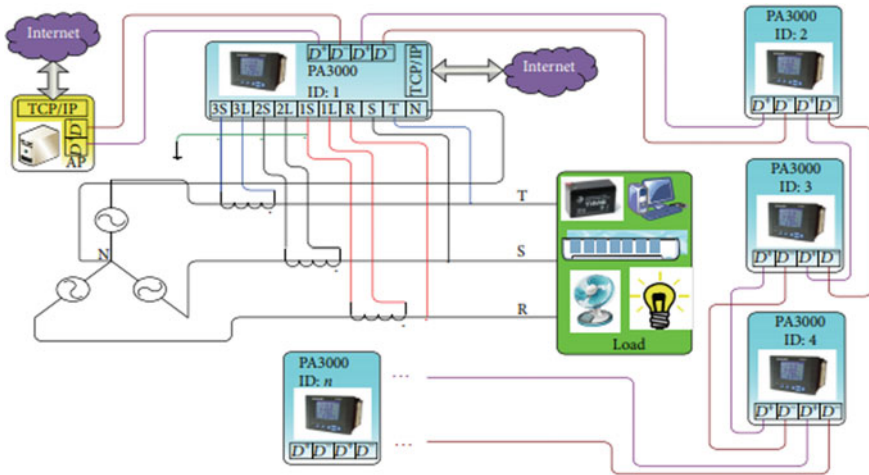


Fig. 1 Hardware system

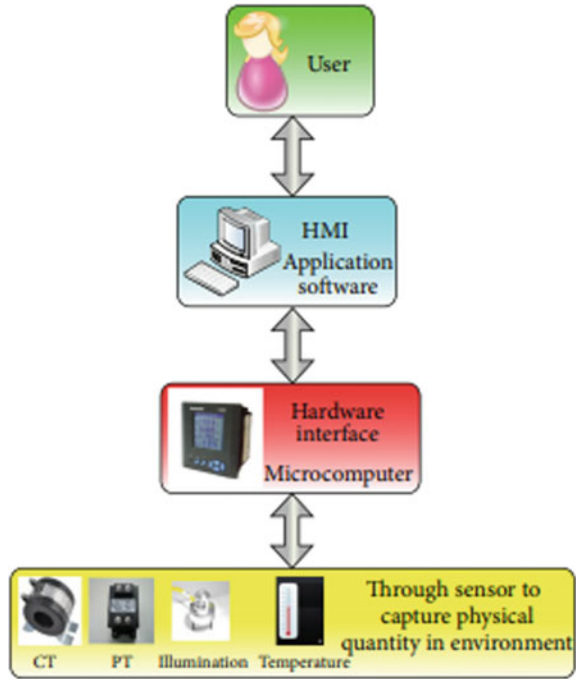
There is an inverter in each module of the system. The communication system to connect several devices to a single network and interact with them simultaneously is required.

A typical industrial communication standard, RS-485, connects up to 32 measurement units over a distance of 1.2 km using the RS-485 protocol. If the transmission gap is more than 1.2 km, RS-485 relay stations ensure that no signal packets are lost. An Ethernet network employing the TCP/IP communication standard to read electric energy data from a distance may be attached to the measuring site’s network. As a result, every piece of Web-based measurement equipment will have its fixed IP address.

2.2 Data Gathering System

The monitoring system is determined by the precision and unity of the acquisition system. Overall success of the project depends on the selection of the appropriate calibrating system and transmission technology. Below is an overview of the data collection process. The analog–digital converter circuit first converts signals from remote sensors into signals with the highest possible resolution and preprocesses them. The digitized raw data are then sent to the microcomputer; Fig. 2 shows the user-machine interface for displaying the search results (see below). The flow diagram for programming is shown in Fig. 3. The COM port has been activated and configured to read data from the COM port every 15 min automatically. When the data are read, the search for missing packets begins, and the integrity of the package

Fig. 2 Data acquisition architecture



is assessed. If there are no problems with the enclosures, the information is uploaded to local and remote databases.

2.3 Data Collecting Process

Distributed modules and an inverter combine to form solar power plants. As a result, the communication system must let several devices communicate over the same network. The Modbus protocol enables a large number of devices on the same Web to interact with each other. As a consequence, Modbus is the data gathering system’s communication protocol of choice. In serial and Ethernet topologies, the Modicon Company’s Modbus protocol is often used.

Since the content of the communication protocol is free of permission fees and simple to operate, it is an excellent option since diverse equipment can quickly comply. As a result, the time and money required to construct a more complex system will be decreased. For the master to get the correct data from each slave throughout the investigation, each measuring system will have its unique address. The architecture as a whole only has one master (the data acquisition system). Everybody else is a Slavic (the measurement systems).

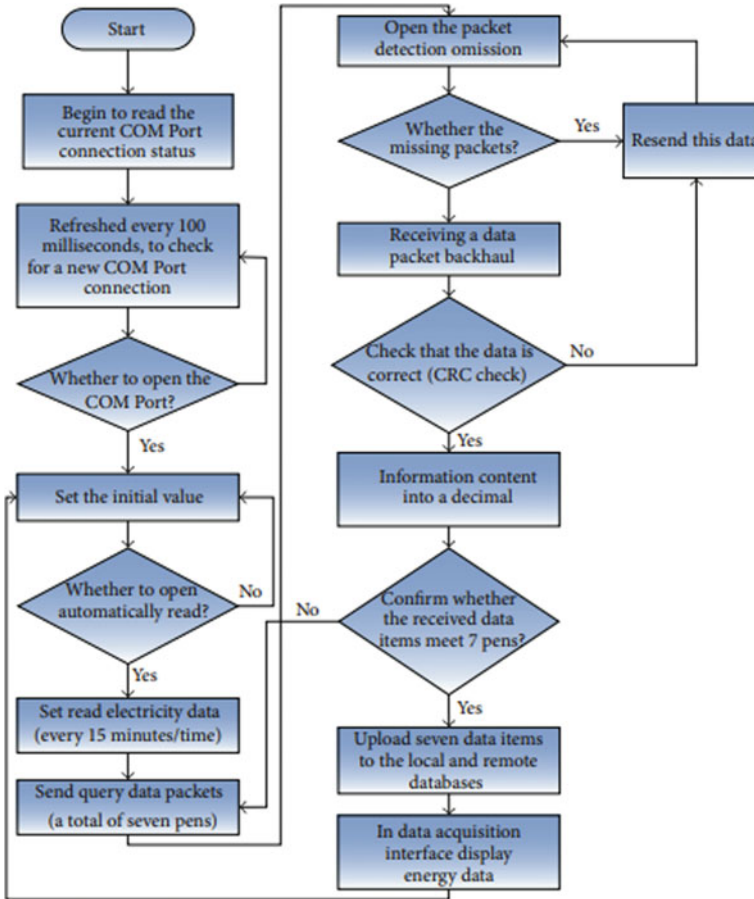


Fig. 3 Data acquisition system flowchart

2.4 Cloud System

On the login page, enter your username and password to connect to the server that manages logins. Credentials for both the user and the administrator are returned after identity has been validated. This gives distinct client-side authority and allows users and administrators to work independently in different places.

A client-side SQL database manages the real-time streaming video server communications of this article. After client-side authorization has been verified in an SQL database, servers can delete the real-time video source provided. As a result, customers have no problem using the video streaming system.

The cloud data center: This cloud-based data center allows you to store data from all over the world while maintaining the ASP. Client-server communication and



Fig. 4 Information interface for three-phase voltage and current and electrical energy

database communication are combined to set up a monitoring system based on the cloud structure. The result looks like a huge data center in the sky.

3 Experimental Analysis

3.1 Data Gathering System Interface

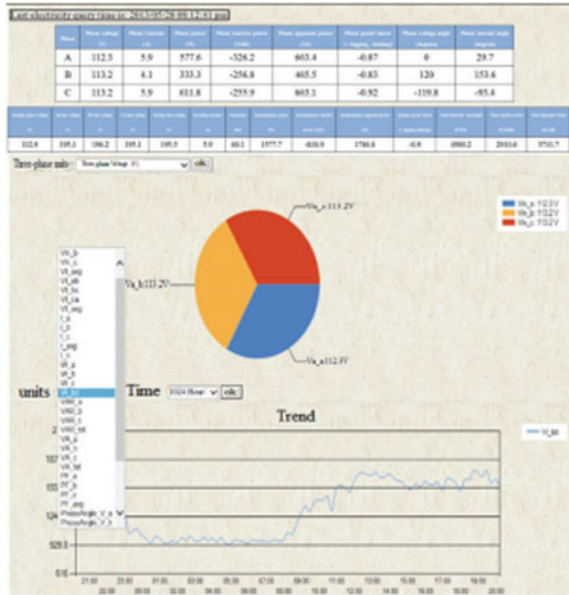
The system’s central monitoring station creates an electric energy data collection program (Fig. 4). Users can immediately start uploading data to the data center using program’s easy-to-learn window software control interface. Examples of tag pages include a harmonic distortion display for three-phase voltage and current and an interface to display 3-phase voltage and electrical power information. All of these features can be found in the software user interface. This gadget uses laboratory power consumption parameters to monitor electricity.

3.2 Cloud System

3.2.1 System for Monitoring Energy Consumption in Real Time

Visually observed electric energy parameters are enumerated and given on the client side, as illustrated in Fig. 5. This plan utilizes two lists. It shows the voltage and current angles for each phase separately on the graph. In addition, the combined active and reactive power of the three steps may be seen in this graph. To put it

Fig. 5 Investigation of power consumption in the laboratory



another way, it shows the three-phase mean or total electric energy characteristics. Identifying data is now easier for users with this new query interface for electrical energy metrics recorded in the past 24 h, three days, or seven days.

3.2.2 Real-Time Video System

Implement real-time monitoring, this system also combines real-time video functions in addition to remote data monitoring. This real-time video capability should be achieved through a streaming server, as shown in Fig. 6. The streaming server collects all real-time video data and sends the data to the computer in the connected network on the client side. The video recording and streaming software are already installed on the streaming server. The encoding technique, bitrate, and scaling for streaming video are all decided when determining the IP address of a streaming server. Click the play button at the bottom of the screen to start streaming the video. When the client is connected to the server over a network to display real-time video, the real-time video system is activated as shown in Fig. 7. When you click on a video to watch it, the server searches the list of the current streaming server’s IP address and port number and passes that information to the client. After receiving the connection data, the client-side master starts searching for and connecting to the source of the video from the streaming server.

Fig. 6 Video capture and streaming program



Fig. 7 Real-time video



3.3 Analysis of Experimental Data for Fault Diagnosis

The illumination of the solar panel is 1000 W/m^2 and decreases according to a given incline. The lighting of a single solar panel is programmed between 100 and 150% of the lighting of the previous eight modules in steps of 15%. Next, let's look at some figures on the use of electrical energy.

The second solar module string is removed and imported into a shading fault discrimination program based on the SVM data format for identification and data output from this system when testing SVM training results. This second chain of solar modules serves as a test object. To describe a typical situation, we would use 100% lighting with 75% brightness, but to illustrate an unusual case, we would use 75% lighting with 0% brightness.

4 Conclusion

A cloud-based monitoring system was developed as a result of this research. For packet communication, the smart meter was connected to a USB-to-RS-485 converter. Electric meter answer packets were analyzed before being divided into two separate bundles. For local use, a database field order is used when uploading data to a data center. The software running on a streaming server may both receive and transmit video content. Encoding techniques, IP addresses, and ports for streaming output are all options. An IP address and port number for the client may be obtained through a server-side database query after a successful connection. The client may then see the real-time video on the server. IIS, ASP.NET, and SQL databases on the cloud are all used in this approach. To ensure that the system runs well, an administration window graphical interface is provided. It may be accessed at any time and from any place in the world. This monitoring system, in contrast to others, is capable of moving across different platforms. Users save time by not reading lengthy texts since it is connected to GIS and provides real-time power usage statistics. As a result, the user will have quick access to accurate information. This system makes it easy for users to see and analyze measured data by emailing or downloading reports and searching primary sources. Table 1 shows how the illumination shading diagnostic procedure uses the SVM theory to provide dependable results.

Table 1 Results

Illumination level	100%	95%	85%	75%	70%	65%	50%	45%	35%
Normal	322/322	322/322	319/320	305/320	4/318	1/319	0/317	1/316	2/315
1st string shaded	0/322	0/322	0/320	0/320	0/318	0/317	0/316	0/315	0/315
2nd string shaded	0/321	0/321	1/320	16/321	314/318	317/319	317/317	315/316	313/316
3re string shaded	0/322	0/322	0/320	0/319	0/317	0/317	0/317	0/315	0/314

References

1. Ranhotigamage C, Mukhopadhyay SC (2011) Field trials and performance monitoring of distributed solar panels using a low-cost wireless sensors network for domestic applications. *IEEE Sens J* 11(10):2583–2590
2. Coleman, Zalewski J (2011) Intelligent fault detection and diagnostics in solar plants. In: *Proceedings of the 6th IEEE international conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS '11)*, Prague, Czech Republic, pp 948–953
3. Iovine J (2017) *PIC microcontroller project book*, 1st ed., McGraw-Hill, pp 35
4. Ibrahim D (2018) *PIC basic projects: 30 projects using PIC BASIC and PIC BASIC PRO*, Elsevier, pp 14–16
5. Mousazadeh H, Keyhani A, Javadi A, Mobli H, Abrinia K, Sharifi A (2009) A review of principle and sun tracking methods for maximizing solar systems output. *Renew Sustain Energy Rev* 13(8):1800–1818
6. Rubio FR, Oretga MG, Gordillo F, Lopez-Martinez M (2007) Application of new control strategy for Sun tracking system. *Energy Convers Manage* 48:2174–2284

Patient Identifier Using Biometric Authentication



N. Ramya, N. Mahika Kamale, M. Darahasa, P. Mahitha, and T. Anuradha

Abstract In case of emergency situations like accidents, the doctor may not have the complete medical history of the patient they are dealing with. This may lead to wrong diagnosis and medical errors, which can even cost a life. “About 2.6 million deaths are caused yearly due to medical mistakes”, said by WHO. Most of which are due to lack of knowledge about the patient’s medical history. This paper proposes a solution which provides the registered users to store and access their medical details in a web application authenticated by username and password. The user details are stored in the form of electronic records. Electronic health records are very useful as they reduce the traditional way of storing patient records where the management may lose some records of patients which can delay the medication of patients. By adopting the use of electronic medical records, medical errors and its adverse effects can be reduced. In severe cases, the victim may not be in a position to brief about his username and password, so the biometric fingerprint authentication is added for the convenience of medical staff to acquire the victim’s medical history. Different medical attributes like blood sugar level, blood pressure, etc. were present alongside the attributes to upload and store X-rays, scan reports, etc. The novelty of the proposed work lies in the implementation of biometric authentication for accessing the EHR. For the fingerprint matching, k-NN algorithm is used in the proposed work. The main motivation behind the proposed work is to reduce improper medications and also proposing a better way to store medical records without losing any record.

Keywords Database · Django framework · Fingerprint authentication · Health records · k-NN algorithm · Web application

N. Ramya · N. Mahika Kamale · M. Darahasa · P. Mahitha · T. Anuradha (✉)
Department of Information Technology, Velagapudi Ramakrishna Siddhartha Engineering
College, Vijayawada, India
e-mail: anuradha_it@vrsiddhartha.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023
S. C. Satapathy et al. (eds.), *Computer Communication, Networking and IoT*,
Lecture Notes in Networks and Systems 459,
https://doi.org/10.1007/978-981-19-1976-3_11

87

1 Introduction

Medical records represent the patient's past medical history which is important for further medication. In case of emergency situations like accidents, the doctor may not have access to the medical history of the patient/victim they are dealing with. Even the patient may not be in a condition to brief about their medical history. "More than 138 million patients are affected by the wrong medical decisions made by doctors due to lack of medical history of the patients", proposed by WHO in the article [1]. With this thought, this proposed work provides a web application where the registered user can store their medical details and their fingerprint image. The user can login to the web application by using the login credentials or by using the fingerprint image. The doctor/hospital staff of the hospital which has registered for the site can have access to the patient's medical details. The application contains attributes like blood sugar level, blood pressure level, skin allergies, etc. along with the attributes where one can upload their X-ray reports, scan reports, etc. in the form of images or files. The user can update his profile by clicking on update profile in the dashboard page. The user can update his details such as age, number, health insurance number and health details. The web application is developed using the Django framework which has a database (db sqlite) in the backend. The application is authenticated by username and password. Biometric fingerprint authentication is also added to the application to properly serve the purpose of giving access of the patient's medical history to the hospital staff/doctor even if the victim is not in a position to brief anything. The fingerprints are taken through a fingerprint scanner and are uploaded to the database in the form of images while registering. In every situation, the patient is not able to use his login credentials always; there will be some emergency cases where the patient will not be able to use his login credentials; and in such cases, fingerprint authentication helps them to share their details. The use of biometric authentication specifies the novelty of the proposed work while there are many EHRs without this feature. So, biometric enumerates the novelty of our proposed work. For the fingerprint matching, k-NN algorithm is used to obtain the accurate results. The users need to update their details in the web application frequently, so that their data is accurate. The proposed work also serves another purpose as electronic health records, which reduces the effort of carrying a pile of medical documents wherever the patient goes.

2 Literature Survey

The proposed work is based on some of the studies and existing applications. From the work proposed by the authors in [2, 3], the basics about electronic health records is taken, as the total proposed work is solely dependent on them. The importance of digitization of health data is known from the author's work in [4]. The basic structure of public health in India and the evolution that happened in storing health data over

the time has been stated by the work in [5, 6]. “EHR is a technological development in healthcare that does away with the traditional paper-primarily based documentation of clinical reports” stated in [7]. There are many advantages of EMR. The effective use of EHRs is stated in [8, 9]. Primarily, it eliminates the need to store and carry paper reports whenever a patient visits a medical doctor. With EMR, practically, they carry their entire healthcare information with them wherever they go. The article [10] gives a view about the EHR developed in India such as MyHealthRecord developed by the Ministry of Health and Family Welfare jointly with the Ministry of Electronics and IT, Govt. of India. The infrastructure of the proposed work is influenced by the similar application in [11]. The importance of patient’s health data being available to the health professionals is stated by the authors in [12]. The blueprint of the development process of the EHR by the Indian government is depicted in the article [13]. The main part of this project is biometric authentication. The fingerprint authentication using Django framework based on Python web biometric authentication is developed using the code in the article [14]. To match the fingerprints, k-NN algorithm is used. The implementation of the k-NN algorithm is shown in the article [15].

3 The Proposed Work

This web application is a type of electronic health record system developed using Django framework which functions as an electronic health record as well as helps the hospital management to get access to the patient’s health details apart from the user only. Bootstrap framework is used to develop the user interface of the application. The database at the backend is the db sqlite, which is used to store all the user details. The novelty of this proposed work lies in the biometric fingerprint authentication.

Figure 1 shows the architecture diagram of the project. This diagram depicts the entire project flow.

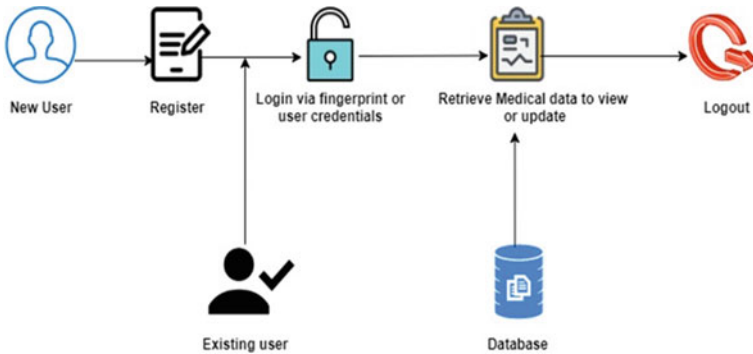


Fig. 1 Architecture diagram

Fig. 2 k-NN algorithm

- 1) Load the data.
- 2) Initialize K to your chosen number of neighbors.
- 3) For each example in the data
- 4) Calculate the distance between the query example and the current example from the data.
- 5) Add the distance and the index of the example to an ordered collection.
- 6) Sort the ordered collection of distances and indices from smallest to largest (in ascending order) by the distances.
- 7) Pick the first K entries from the sorted collection.
- 8) Get the labels of the selected K entries.
- 9) If regression, return the mean of the K labels.
- 10) If classification, return the mode of the K labels.

If the user is a new one, then he/she needs to first register himself/herself to the application. While registering, the user needs to provide a lot of their details along with their username, password and fingerprint through which they can login to the application from next time. The fingerprint is taken through the fingerprint scanner and is uploaded as an image into the database. Once registered, the user gains the permissions of a registered user and becomes an existing user. If an existing user wants to login to the application, they should provide their username and password or simply their fingerprint. If the details provided by the user are valid, the user will be successfully logged in to the application, where the user can view or update their medical details. Once logged in, the existing details of the particular user are retrieved from the database and can be seen by the user in the home page of the application. Once the user is done viewing or updating his/her details, he/she can successfully logout of the application by simply clicking on the logout button.

Here, the k-NN algorithm is used for fingerprint detection. Figure 2 shows the steps of the k-NN algorithm.

The value of k is taken as 5, so that there are 5 nearest neighbours to be compared. When a fingerprint is given for logging in, the given fingerprint is compared with the nearest five neighbour finger print images stored in the database. If it matches, then the details adhering to that particular fingerprint are retrieved or else the login of the user fails.

4 Experimental Results

In the proposed application using biometric authentication, any registered user can login via two ways. The first way is to use the credentials like username and password. The other way is to use the fingerprint as a unique identifier, which will be very helpful when the victim is not in a position to brief about their past medical details. Figure 3 displays the login page with options for non-finger print and finger print-based login. In the first option, users can login using authorized username and

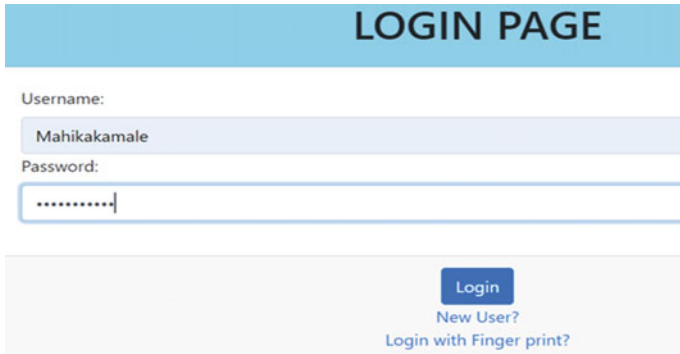


Fig. 3 Login page

password. If the user selects login with fingerprint option, then he will get an alert message to upload his fingerprint message as shown in Fig. 4. If the uploaded fingerprint image matches with the registered one, then successful login takes place and displays the message “fingerprint matched” as shown in Fig. 5. Otherwise, the login is unsuccessful and a message “Fingerprint doesn’t match” is displayed and the user can again try uploading another image as in Fig. 6.

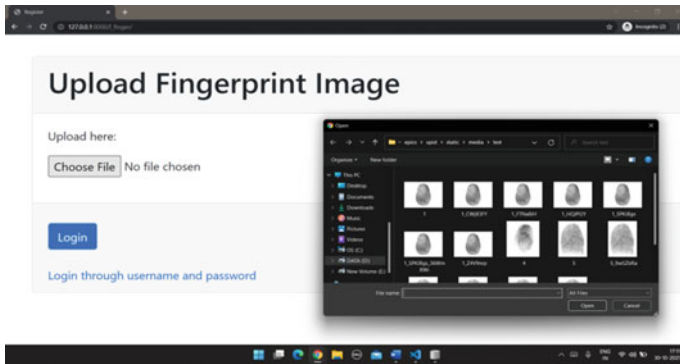


Fig. 4 Login with fingerprint

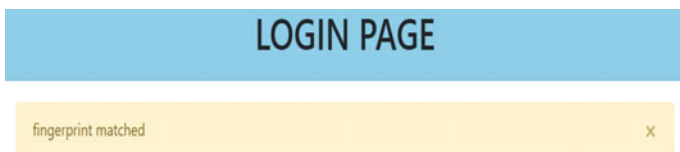


Fig. 5 Fingerprint matched

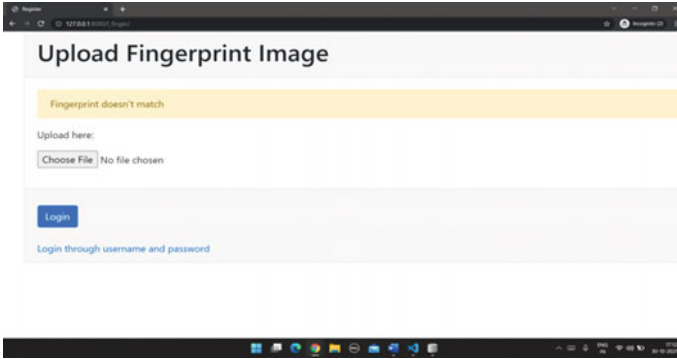


Fig. 6 Fingerprint mismatched

Once the login is successful, the user will be redirected to the homepage where the user gets a dashboard displaying their details and options to update details and add a report. Under update details option, the user can update their details entered at the time of registration. The user can add any medical reports as shown in Fig. 7. Here, the user can select the type of report from the drop down menu and upload the corresponding file.

Table 1 shows the sample records of the registered users' personal details database. Each user is identified by a unique id. Table 2 depicts the view of the database which stores all the medical details of the registered user. User id is used as foreign key to retrieve corresponding medical details of a user.

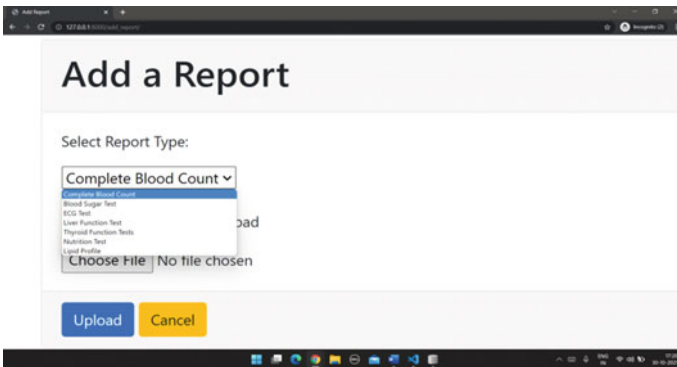


Fig. 7 Add a report

Table 1 Personal details schema

Id	Full name	Age	Gender	Ph. No.	Aadhar	Fingerprint	Username
1	Mahika Kamale	20	Female	799*****	4089***	Ímg.jpg	mahika

Table 2 Medical details schema

Id	Blood group	Allergy	Sugar level	Blood pressure	X-ray	Surgical reports
1	O+ ve	Allergic to abilify	–	Normal	Xray.jpg	No

5 Conclusion and Future Work

Patient identifier using biometric authentication is a web application developed using the Django framework, which has a database (db sqlite) at the backend to store the user details. The proposed work serves two purposes. The main purpose is the retrieval of the patient’s details by the medical professionals using the fingerprint of the patient whenever necessary. The other purpose is to store the medical details of the user and to access them whenever or wherever necessary. This avoids the effort of carrying a pile of records wherever the user goes. The main motto of this work is to decrease the medical errors due to the lack of proper medical history of a patient.

The current work can be further extended by providing more security measures as the proposed work deals with the health data, which is sensitive. Furthermore, the addition of features like face detection can be implemented to simplify the access of the data.

References

1. WHO (2019) Medical errors due to improper health details. <https://www.indiatoday.in/world/story/medical-mistakes-cause-2-6-million-deaths-yearly-who-1599019-2019-09-14>
2. Lindrud SD (2015) The evolution of the electronic health record. <https://pubmed.ncbi.nlm.nih.gov/25840379/>
3. Gold M, McLaughlin C (2016) Assessing hitech implementation and lessons: 5 years later. *Milbank Q* 94(3):654–687
4. Balsari S, Fortenko A, Blaya JA, Gropper A, Jayaram M, Matthan R, Sahasranam R, Shankar M, Sarbadhikari SN, Bierer BE et al (2018) Reimagining health data exchange: an application programming interface-enabled roadmap for India. *J Med Internet Res* 20(7):e10725
5. Chokshi M, Patil B, Khanna R, Neogi SB, Sharma J, Paul V, Zodpey S (2016) Health systems in India. *J Perinatol* 36(3):S9–S12
6. Gopal KM (2019) Strategies for ensuring quality health care in India: experiences from the field. *Indian J Commun Med Off Publ Indian Assoc Prev Soc Med* 44(1):1
7. P. O. of Science and Technology (2016) Electronic health records. <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0519>
8. Banff (2015) Adoption and effective use of digital health across Canada. <https://www.inforoute.ca/en/component/edocman/resources/i-infoway-i-corporate/annual-reports/2771-annual-report-2014-2015>
9. Kruse CS, Stein A, Thomas H, Kaur H (2018) The use of electronic health records to support population health: a systematic review of the literature. *J Med Syst* 42(11):214
10. National Health Portal, Ministry of Health and Family Welfare, Government of India, EHR Standards (2016) [Online]. Available: <https://www.nhp.gov.in/NHPfiles/EHR-Standards-2016-MoHFW.pdf>

11. Basu D (2017) The electronic health records system in the UK. <https://www.centreforpublicimpact.org/case-study/electronic-health-records-system-uk/>
12. Ganiga R, Pai RM, Pai MM, Sinha RK et al (2020) A preliminary study of real-time capturing and sharing of routine health data among the public health professionals. *Indian J Community Med* 45(2):176
13. Ministry of Health and Family Welfare, Government of India, Draft National Digital Health Blueprint (2019) [Online]. Available: https://main.mohfw.gov.in/sites/default/files/Final%20DHB%20report_0.pdf
14. Idogun J (2021) Fingerprint-based authentication and authorization in Python (Django) web applications. <https://dev.to/sirnej/fingerprint-based-authentication-and-authorization-in-python-django-web-applications-2c61>
15. IEEE (2014) Graph based K-nearest neighbor minutiae clustering for fingerprint recognition. <https://ieeexplore.ieee.org/document/6975917/references#references>

Recognition of Hand Gesture-Based Sign Language Using Transfer Learning



B. Lakshmi Ramani, T. Sri Lakshmi, N. Sri Durga, Shaik Sana, T. Sravya, and N. Jishitha

Abstract Sign languages are the natural languages of the deaf and dumb community and provide access to communication. The discipline of sign language recognition and translation is exploding. Hand gesture-based sign language recognition is a fortunate application of human–computer interaction. A developed model detects sign language gestures involving feature extraction and classification. This work presents transfer learning-based image recognition models using VGG16 and ResNet50 to translate static hand gestures into text with 57 gesture classes. Fine-tuning hyper-parameters of VGG16 and ResNet50 are used to further improve image recognition accuracy. The test results are compiled and evaluated on the large-scale dataset and showed that the recognition rate was significantly improved compared with Support Vector Machine, Random Forest, Logistic Regression, and XGBoost.

Keywords Sign language · Static hand gestures · Gestures recognition · VGG16 · ResNet50 · Image classification

1 Introduction

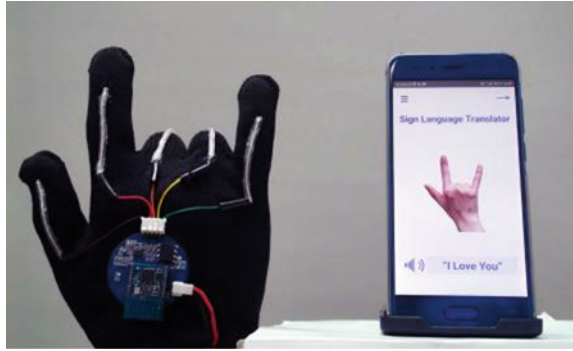
Communication is essential for a long time in the environment. Communication amongst all members of the community, especially the deaf, creates deeper understanding. The majority of communication in the current circumstance has taken place through vocal sounds and body language gestures. While vocal sounds are important in conversation, other aspects of body language, such as emotions, are essential.

The deaf and dumb community's leading social issues are the communication barrier and the hearing majority, which prohibit them from obtaining essential life services. The skill of non-verbally communicating our thoughts and feelings is known

B. Lakshmi Ramani (✉) · T. Sri Lakshmi · N. Sri Durga · S. Sana · T. Sravya · N. Jishitha Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India
e-mail: blramani@pvpsiddhartha.ac.in

T. Sri Lakshmi
e-mail: tslakshmi@pvpsiddhartha.ac.in

Fig. 1 Sensor-based



as sign language and is the deaf and dumb community’s principal mode of communication. Because the world’s deaf and dumb population numbers over 90 million individuals, proper sign language interpretation is crucial, so they use a range of hand gestures to communicate. The two most common methods for recognizing sign languages are (i) sensor-based and (ii) image-based.

1.1 Sensor-Based

The sensor-based technique employs instrumental gloves with sensors to detect hand articulates, as shown in Fig. 1. The angles and positions of each joint in a user’s movements have been collected using wearable data gloves. The difficulty and expense of building a wearable sensor have limited its use.

1.2 Image-Based

The image-based technique employs cameras to capture an image sequence of the signer making the sign and then image processing to detect the actions, depicted in Fig. 2.

Human hand gesture recognition is becoming highly useful in sign language recognition, video monitoring, robot control, virtual gaming, and home automation [1]. A hand gesture is an expressive communication strategy used in the entertainment, healthcare, and education industries to help people with special needs [2]. Hand tracking is required for hand gesture identification and entails a variety of computer vision operations such as detection, hand segmentation, and tracking.

In this work, we are dealing with image-based recognition. Non-contact visual examination-based gesture recognition systems are now widely used. This is due to the ease and low cost to the user.

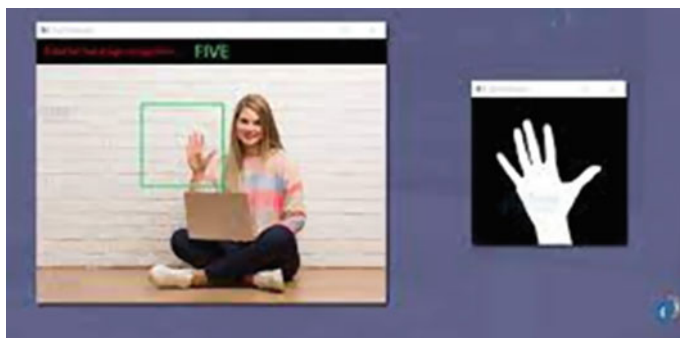


Fig. 2 Image-based

Accurate hand gesture detection remains a significant issue for most recently developed recognition algorithms. Deep learning (DL)-based hand gesture identification systems can deliver promising results due to the recent advancement of deep neural networks (DNN) and their good performance [3]. The technology recognizes and grasps different human gestures, making human-machine communication more successful.

This work aims to develop a recognition system of static hand gestures that translates the gestures of a sign into text, the most important part of sign language vocabulary. The gestures dataset used in this study is accessible for free on Kaggle. The dataset includes all the digits, alphabets, and some daily actions like Call, Cold, OK, Single, etc. The models VGG16 and ResNet50 were used to train the dataset in this work. Some of the hyperparameters were fine-tuned to enrich the accuracy of the model.

2 Literature Review

The authors suggested a static hand gesture recognition model based on geometry. The primary goal of this study is to create a vision-based system for recognizing static hand motions, which is a low-cost solution and is limited to tiny datasets only [4].

Hand gesture recognition model using convexity hull defects to control an industrial robot, proposed by the authors [5]. This work aims to control an industry robot using the gestures of a hand. The dataset contains the five digits (1, 2, 3, 4, 5). It includes Convex Hull and Convexity Hull Defects algorithms. The experimental results show a limitation in finger count recognition accuracy, and poor lighting affects gesture recognition.

The author presented research work, namely hand gesture recognition for the disabled using convolutional neural networks (CNNs) and implementation. The central target of this work is to recognize the gestures of a hand by using the CNN

algorithm. CNN networks with convolutional, pooling, dense sequence layers are located. The dataset consists of various symbols and some actions. The model handles static hand gestures provided by any person and help to identify what type of gesture it is [6].

The author has proposed an automated hand gesture recognition using a deep convolutional neural network (DCNN) model. The author aims to use gesture recognition technology to build an algorithm to categorize photographs of diverse hand motions and signs. Real-time anti-encroaching hand gesture identification and hand tracking mechanisms were utilized in this study, which improved human–computer interactions and simplified day-to-day communication [7].

An efficient hand gesture recognition system is presented based on DCNN by the authors [8]. This study aims to deploy a camera to monitor the region of interest (ROI) in an image, as the hand area, which recognizes the hand motions for home appliance control or human–computer interaction. The image is scaled before being fed to a CNN to recognize numerous hand gestures. The two CNN’s AlexNet and VGGNet employed the technique kernelized correlation filters (KCF) [8].

The authors proposed a brief review of the recent trends in sign language recognition. This research examines several techniques to feature extraction methods, sign identification, classification methods, and so on. It resolves the difficulties, limitations, and possibilities for automatic gesture recognition. Because of the system’s limitations and the wide range of hand shapes, pre-processing constantly evolves to discover the most precise solutions [9].

3 Materials and Methods

3.1 Dataset

In the collection of hand gesture datasets, there are 57 gestures with digits, alphabets, and actions which depict in Fig. 3a–c. Actual creative images of hand gestures were collected from several people with various directions of 57 gestures, all of which were captured against a range of surroundings with varying degrees of illumination. The dataset contains 46,700 images, with 41,500 used for training and 5200 images used to evaluate the CNN’s recognition accuracy.

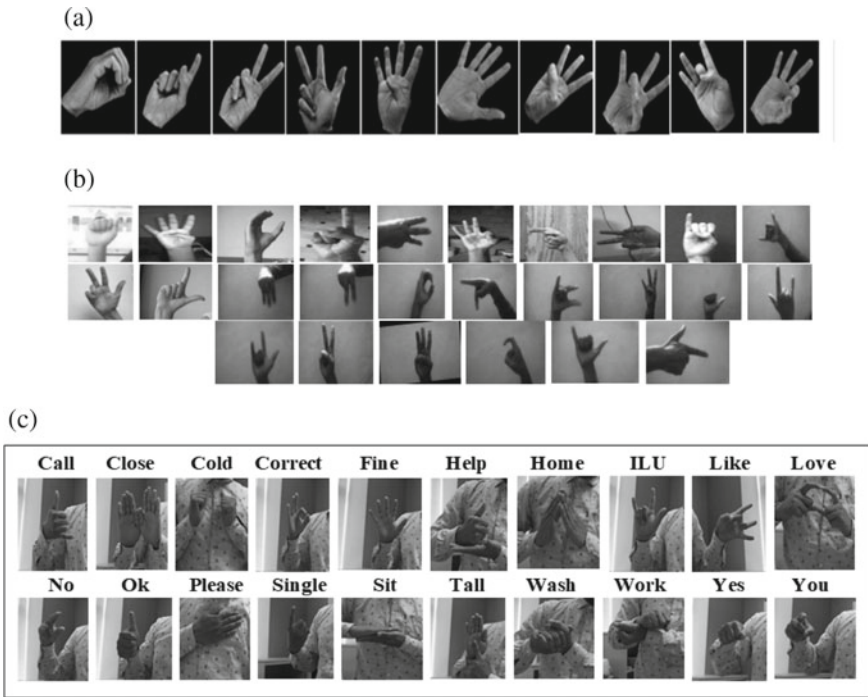


Fig. 3 a Digits. b Alphabets. c Action

3.2 Methodology

In the training phase, the state-of-the-art models VGG16 and ResNet50 are utilized to determine which gesture type the input image matches. In this process, first pre-process the input gesture images, and the second is to train the model.

Pre-process Stage

To decrease computational complexity and improve performance, minimal pre-processing is conducted on the dataset. Initially, the larger size images can be resized to the required fixed size and fed to the model. Reduction of image size means less distortion of the image’s features and patterns, which impact deformations on classification accuracy. As a result, deciding on a fixed image size involves a trade-off between computing efficiency and accuracy.

Training Stage

This phase includes two stages: Extracting the features and classification.

Extracting the features.

Feature extraction is a process in dimensional reduction, which reduces an extensive collection of raw data into smaller groups. These enormous data sets include a large

number of variables and are the most crucial feature. A large amount of computational power is required to handle these variables. As a result, feature extraction aids in the extraction of the best feature from large data sets by selecting and combining variables into features, thereby lowering the quantity of data. These characteristics are simple to use while still accurately and uniquely describing the actual data set.

Classification.

In terms of CNN, the fully connected layer is a classification layer. This phase classifies the images and uses the Softmax activation function, which predicts a multinomial probability distribution. The label which is having the maximum probability will become our output gesture.

Transfer Learning

Transfer learning is a deep learning approach in which a CNN trained for one task is used to build a model for a second task [10]. This is due to the fact that deep learning architectures require a lot of time and computational resources to train huge parameters, and obtaining a large labelled dataset for model training is a complex process. As a result, transfer learning has become the preferred method increasingly and is instinctually used in practical applications, namely solutions based on the use of a pre-trained network where only the parameters of the final classification layers must be inferred from scratch using the training set [11, 12].

VGG16.

The VGG-16 is a 16-layer convolutional neural network. Compared to AlexNet, this network substitutes huge kernel-sized filters with numerous 3x3 kernel-sized filters one after the other, followed by Max-pooling across a 2x2-pixel window with stride two and three completely connected layers. Image recognition, classification, detection, and localization are all possible with VGG16.

ResNet.

ResNet, a 50-layer neural network, was successfully trained using the ResNet unit. Compared to neural networks with simple layers, ResNet significantly improved the performance of neural networks with extra layers. The concept of residual learning is presented, and it is shown to be effective in dealing with network degeneration. It produces good results despite having fewer parameters than VGGNet. 3.57% of the time, the error rate is 3.57%.

4 Experimental Results

The work employed the VGG16 and ResNet50 and was trained and tested on the gestures data. The predictions on test data and the model's efficiency are observed by increasing the number of epochs. Evaluated and compared the accuracies of the model with the test dataset. Throughout testing, the best model from the training

Table 1 Training phase parameters

Parameters	VGG16	ResNet50
Activation	ReLu, Softmax	ReLu, Softmax
Optimizer	Adam	Adam
Loss	Categorical cross-entropy	Categorical cross-entropy
Epochs	10	10
Batch size	64	64
Learning rate	3e-4	3e-4

phase is utilized. The model predicts the gestures of all input images from the test set. With the predicted and actual output given in the dataset, accuracy has been calculated.

Table 1 shows the various parameters used for the models VGG16 and ResNet50. Adam optimization algorithm is used, learning rate with 0.0001 is fixed, batch size of 64 with five epochs were utilized.

First, the experimentation uses VGG16 to recognize hand gestures. Figure 4a indicates the accuracy, and Fig. 4b depicts the loss curves of the model. The experimental test accuracy reaches 90.78%, and the loss is 0.43%.

Using ResNet50 to recognize the hand sign gestures, the test accuracy of the model has achieved 94.13%. Figure 5 shows the model accuracy and loss curves.

Table 2 shows the comparison of the VGG16 and ResNet50 models. The model ResNet achieves better accuracy when compared to VGG16 with the hand gesture alphabets, digits and actions.

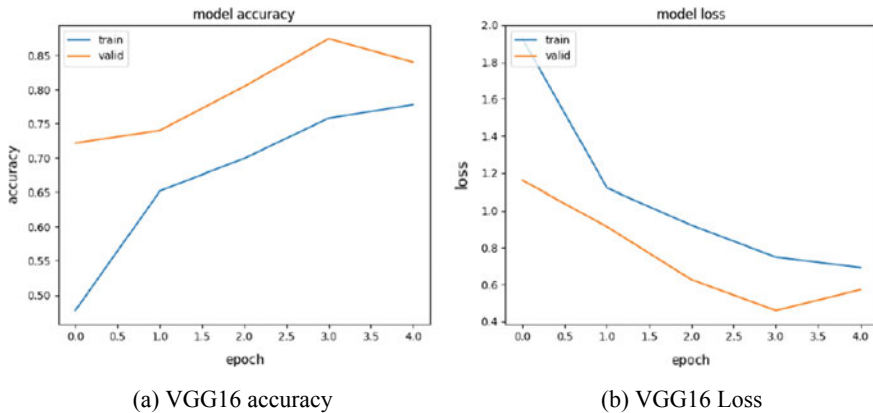


Fig. 4 VGG16 model accuracy and loss

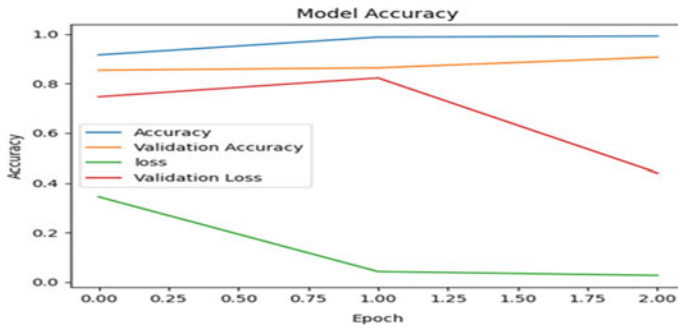


Fig. 5 ResNet50 model accuracy and loss

Table 2 Comparison of models

Model	Classes	Accuracy (%)
ResNet50	57	94.13
VGG16	57	90.78

5 Conclusion

In this work, the capability of a deep learning technology was used to recognize hand gesture positions from the images. To minimize the complexity of gesture recognition, we introduced VGG16 and ResNet50 models with a pre-processing layer. The system’s main advantage is that it eliminates the need to create a model for each move based on hand properties like fingers and curves. To reduce the training time of the CNN model is after pre-processing, the duplicate information in gesture images is removed, and background information is cleared. The models were trained to learn 57 gestures. For training and testing, the model, the number of images 41,500 and 5200, were used. The evaluation was performed for the models with good accuracy, whereas the ResNet50 achieves better accuracy when compared to VGG16. We may deduce from the models that it can manage some hand gestures made by anyone and assist us in identifying the gesture. So the essential element to consider is that the machine can interpret and decide what the images are, which is beneficial in various ways.

References

1. Sagayam KM, Jude Hemanth D (2017) Hand posture and gesture recognition techniques for virtual reality applications: a survey. *Virtual Reality* 21(2):91–107
2. Cheok MJ, Omar Z, Jaward MH (2019) A review of hand gesture and sign language recognition techniques. *Int J Mach Learn Cybern* 10(1):131–153
3. Ramani BL, Tumuluru P (2019) Deep learning and fuzzy rule-based hybrid fusion model for

- data classification. *Int J Recent Technol Eng* 8(2):3205–3213
4. Nguyen T-N et al (2014) Geometry-based static hand gesture recognition using support vector machine. In: 2014 13th International conference on control automation robotics & vision (ICARCV). IEEE
 5. Ganapathyraju S (2013) Hand gesture recognition using convexity hull defects to control an industrial robot. In: 2013 3rd International conference on instrumentation control and automation (ICA). IEEE
 6. Varun KS, Puneeth I, Prem Jacob T (2019) Hand gesture recognition and implementation for disables using CNN'S. In: 2019 International conference on communication and signal processing (ICCSP). IEEE
 7. Dhall I, Vashisth S, Aggarwal G (2020) Automated hand gesture recognition using a deep convolutional neural network model. In: 2020 10th International conference on cloud computing, data science & engineering (confluence). IEEE
 8. Chung H-Y, Chung Y-L, Tsai W-F (2019) An efficient hand gesture recognition system based on deep CNN. In: 2019 IEEE International conference on industrial technology (ICIT). IEEE
 9. Nimisha KP, Jacob A (2020) A brief review of the recent trends in sign language recognition. In: 2020 International conference on communication and signal processing (ICCSP). IEEE
 10. Lumini A, Nanni L (2019) Deep learning and transfer learning features for plankton classification. *Ecol Inform* 51:33–43
 11. Kessentini Y, Besbes MD, Ammar S, Chabbouh A (2019) A two-stage deep detection and recognition. *Expert Syst Appl* 136:159–170
 12. Subramanian M, Narasimha Prasad Lv (2021) Hyperparameter optimization for transfer learning of VGG16 for disease identification in corn leaves using Bayesian optimization. *Big Data*

Robustness Indices of 3R and 4R Planar Serial Manipulators with Fixed Actuation Scheme



Shaik Himam Saheb and G. Satish Babu

Abstract The applications of automation and robotic manipulators are evidently increasing due to many advantages; this paper presents the planar serial manipulator performance analysis. There are many performance indices to explain the suitability and selection of manipulators; in this analysis, the Robustness Index-I and Robustness Index-II are considered for 4R and 3R manipulators. The 4R and 3R planar serial manipulators are taken in planar condition as the moment is restricted to a single plane. The 4R and 3R manipulators have all joints with revolute type in nature, and the actuations are arranged at the fixed base joint, the manipulators are provided with base actuation which is fixed. The link lengths of the manipulator are varied in different ratios and the performance evaluation is conducted, and these indices are calculated with the help of Jacobian matrix. Direct kinematic relations were used to generate the Jacobian matrix.

Keywords Performance measures · Serial manipulators · Robustness Index-I, Robustness Index-II · Different kinematic link lengths

1 Introduction

According to the physical appearance of a robot, the most of robots can be taken as the humanoid robots, a numerically controlled machine, a walking machine or a humanoid of science fiction. In industry, most robots are mechanical manipulators instead of humanoids in appearance. Considering that, a mechanical manipulator is a mechanism, and the terms “robot,” “manipulator,” “mechanism” and “robotic manipulator” often refer to the similar kind of terms in the robotics community.

S. H. Saheb (✉)

IcfaiTech (Faculty of Science and Technology), The ICFAI Foundation for Higher Education, Hyderabad, India

e-mail: Himam.mech@gmail.com

G. Satish Babu

Department of Mechanical Engineering, JNTUHCEH, Hyderabad, India

The fundamental structure of a manipulator is the open kinematic chain or serial manipulator. From a topological point of view, a kinematic chain is expressed as the number of links is connected in such that the first link is connected to final (last) link to transfer the defined motion [1]. The articulation between two consecutive links can be realized by means of either prismatic or revolute joint. In an open kinematic chain, prismatic or revolute joint provides the structure with single degrees of freedom (DOF). Revolute joints are preferred than the prismatic joints because of frictional forces, and the revolute joints generate less friction as compared to prismatic joints and also the compactness and reliability of revolute joints [2, 3]. Due to implementation of loop constraints in a closed kinematic chain, the possible DOF is less than the number of joints [4].

In general, sense of a task consisting of arbitrarily pose which means position and orientation an object in the spatial system, six DOF and three DOF for positioning a point on the object and another three DOF for orientation of the end effector, the object with respect to a reference coordinate frames. The Degrees of Freedom of any manipulator is more than the required degrees of freedom then that manipulator is called redundant manipulators [5–7]. The manipulator performance is calculated based on Jacobian matrix, and then, there are many performance measures which are proposed, in this papers, the robustness indices are considered for evolution [8].

Cylindrical jointed robots are different as compared with Cartesian jointed robots as the major differences are degrees of freedom and joint force losses [9]. Cylindrical jointed robot had best mechanical stiffness characteristics. These robots has hollow cylindrical workspace and these manipulators are best suited for pick and place, and other applications are the cylindrical joints of the robot manipulator have less friction characteristics as compared to prismatic jointed robot [10].

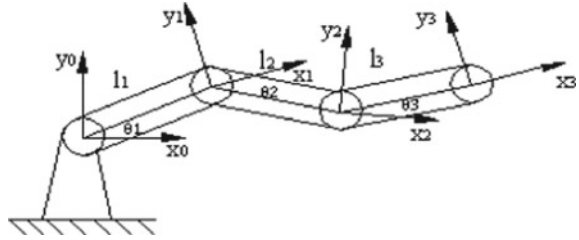
The serial arm robots consist of two major driving forces that are inertia forces and friction forces inertia forces which depends on the mass of the body and the acceleration associated with that mass, these pseudo forces creates critical vibration issues [11]. Like other geometrical scaling, the robot is not possible to scale directly to micro robot as the scaling of micro robot may cause unbalanced inertia forces [12]. This concludes that serial arm manipulators are not much suitable for path planning operations or to manipulate heavy loads and also have poor positioning.

2 Mathematical Modeling and Jacobian Matrix of Planar 3R Serial Manipulator

The Jacobian matrix expressed with respect to the coordinate frame located at the manipulator tip (third coordinate frame) is given by (Fig. 1)

$${}^3J = \begin{bmatrix} l_2s_3 + l_1s_{23} & l_2s_3 & 0 \\ l_2 + l_2c_3 + l_1c_{23} & l_3 + l_2c_3 & l_3 \\ 0 & 0 & 0 \end{bmatrix}$$

Fig. 1 Kinematic model of planar 3R serial manipulator



Considered 3×3 Matrix then

$$T_{3 \times 3} = \begin{bmatrix} r_1 & 0 & 0 \\ e_{21}r_2 & r_2 & 0 \\ e_{31}r_3 & e_{32}r_3 & r_3 \end{bmatrix}$$

$$\text{Det of } [T] = r_1r_2r_3$$

$$\text{Adj}[T] = \begin{bmatrix} r_2r_3 & -e_{21}r_2r_3 & e_{21}e_{32}r_2r_3 - r_2r_3e_{31} \\ 0 & r_1r_3 & -r_1r_3e_{32} \\ 0 & 0 & r_1r_2 \end{bmatrix}$$

$$T^{-1} = \frac{\text{Adj}[T]}{\text{Det}[T]}$$

$$T^{-1} = \frac{1}{r_1r_2r_3} \begin{bmatrix} r_2r_3 & 0 & 0 \\ -e_{21}r_2r_3 & r_1r_3 & 0 \\ r_3r_2(e_{21}e_{32} - e_{31}) & -e_{32}r_1r_3 & r_1r_2 \end{bmatrix}$$

$$T^{-1} = \begin{bmatrix} \frac{1}{r_1} & 0 & 0 \\ -\frac{e_{21}}{r_1} & \frac{1}{r_2} & 0 \\ \frac{e_{21}e_{32} - e_{31}}{r_1} & -\frac{e_{32}}{r_2} & \frac{1}{r_3} \end{bmatrix}$$

3 Performance Indices of the 3R Planar Serial Manipulator

The performance indices of the manipulator play a major role to select the type of robot for any specific application as some applications demands more workspace, compromised repeatability but in some specific applications, the precise positioning is a key parameter, whereas workspace and other parameter values are takes as compromised values. The Robustness Index-I and Robustness Index-II are calculated for 3R and 4R manipulator with different link lengths, as the changes in the link length lead to change of performance, for example, the increase in link length of a serial robot leads to poor stiffness, and the performance indices of the manipulator are

calculated on the basis of the Jacobian matrix of the robot. MATLAB program is used to find the following performance measures.

4 Results 3R Serial Manipulator

The performance indices are evaluated for 3R manipulator with the help of Jacobian matrix; the 3R manipulator consists of three kinematic links that are connected with three revolute joints; these revolute joints are generally referred as 3R robot; and the 3R planar robot has three degrees of freedom. From the direct kinematic relations, the relation between joint angles and link lengths was derived and the relation is referred as Jacobian matrix; the performance analysis is calculated for the proposed planar 3R manipulator, as part of performance analysis, the Robustness Index-I of different link lengths is considered and the RI index values are calculated and plotted as shown in Figs. 2, 3 and 4, similarly, the Robustness Index-II values also calculated for different link lengths and plotted in Figs. 5, 6 and 7. To get the robust solution to any robotic problem, this robustness index gives the variation in the joint spaces. This performance indices are proposed and used by Angeles [13], Ting and Long [14], the double norm or Euclidian norm used by various researchers Zhu and Ting [15] some of researchers are used condition number which is the ration of maximum or largest singular value to the smallest singular value of the matrix. The Robustness Index-I also gives the same meaning as condition number as mathematically both are same, and the Robustness Index-II is defined as the maximum value of the singular value decomposition of the Jacobian matrix. The SVD of matrix can be calculated by any computational software tool; in the current analysis, the MATLAB is used; the SVD of matrix is three-row one-column matrix, and the maximum value of the matrix is referred as the Robustness Index-II (Fig. 7).

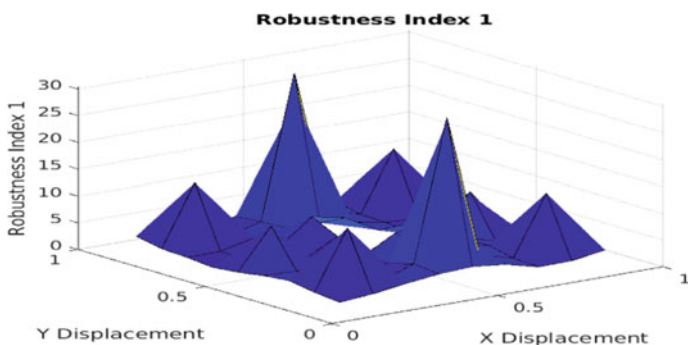


Fig. 2 Variation of Robustness Index-I for a 3R-manipulator (Condition-I the link lengths taken as one unit and the angles are increased with increment of 10°)

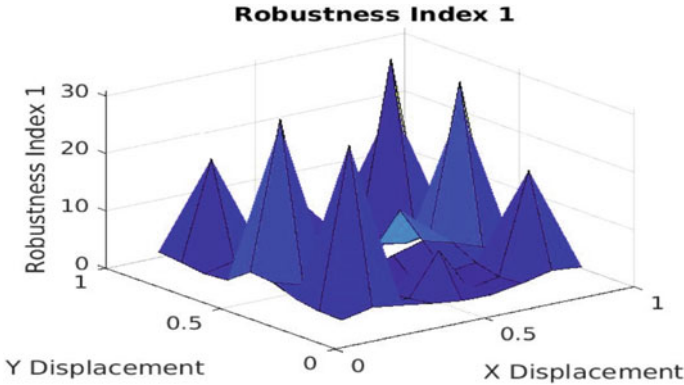


Fig. 3 Variation of Robustness Index-I for a 3R-manipulator (Condition-II the first link length taken as 2 unit, second link length as 1 unit and third link length as 0.5 unit, the angles are increased with increment of 10°)

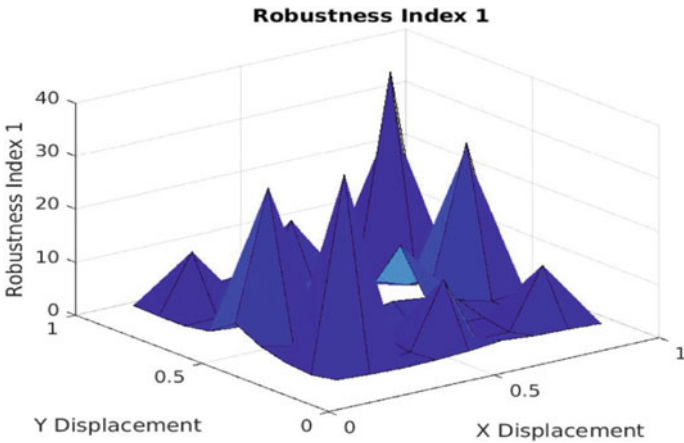


Fig. 4 Variation of Robustness Index-I for a 3R-manipulator (Condition-III the first link length taken as 2 unit, second link length as 1.5 unit and third link length as 0.5 unit, the angles are increased with increment of 10°)

5 Planar 4R Serial Manipulator

The Jacobian matrix expressed with respect to the coordinate frame located at the manipulator tip (fourth coordinate frame) is given by (Fig. 8)

$${}^4 J = \begin{bmatrix} l_3 s_4 + l_2 s_{34} + l_1 s_{234} & l_3 s_4 + l_2 s_{34} & l_3 s_4 & 0 \\ l_4 + l_3 c_4 + l_2 c_{34} + l_1 c_{234} & l_4 + l_3 c_4 + l_2 c_{34} & l_4 + l_3 c_4 & l_4 \end{bmatrix}$$

consider 4×4 matrix

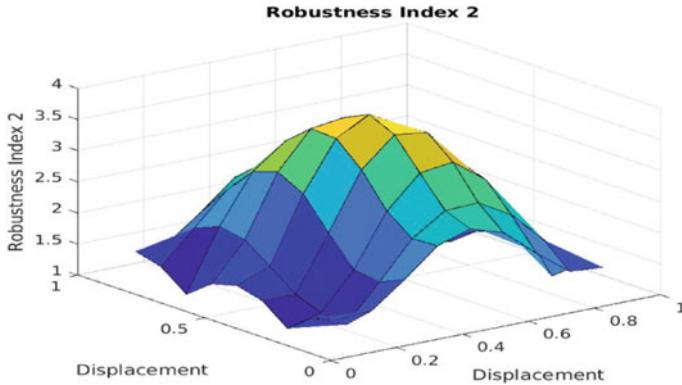


Fig. 5 Variation of Robustness Index-II for a 3R-manipulator (Condition-I the first link length taken as 1 unit, second link length as 1 unit and third link length as 1 unit, the angles are increased with increment of 10°)

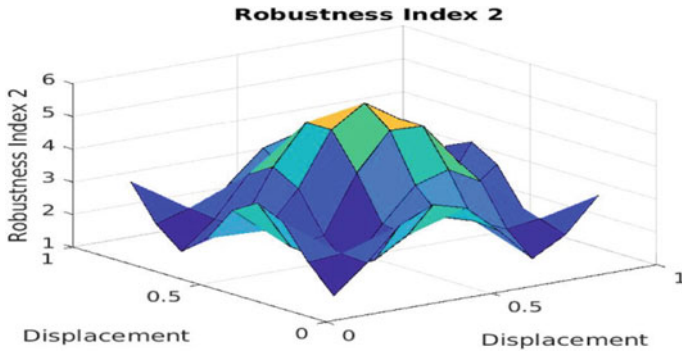


Fig. 6 Variation of Robustness Index-II for a 3R-manipulator (Condition-II the first link length taken as 2 unit, second link length as 1 unit and third link length as 0.5 unit, the angles are increased with increment of 10°)

$$T_{4 \times 4} = \begin{bmatrix} r_1 & 0 & 0 & 0 \\ e_{21}r_1 & r_2 & 0 & 0 \\ e_{31}r_3 & e_{32}r_3 & r_3 & 0 \\ e_{41}r_4 & e_{42}r_4 & e_{43}r_4 & r_4 \end{bmatrix}$$

Determinant of (T) matrix is $= r_1 r_2 r_3 r_4$.

Inverse of matrix $T_{4 \times 4}$ matrix

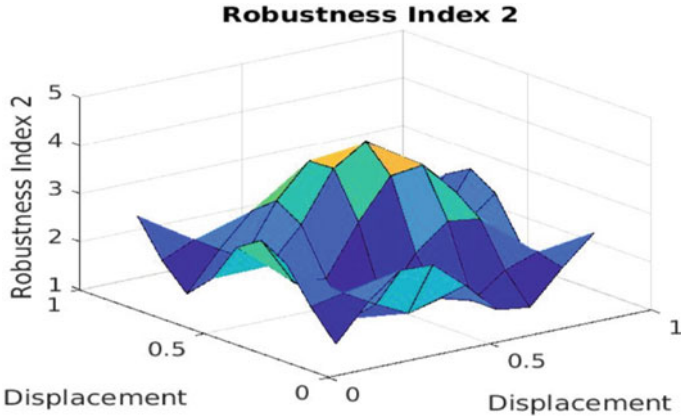
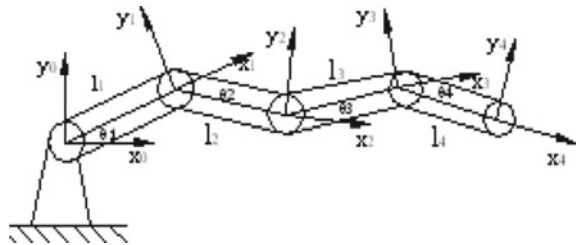


Fig. 7 Variation of Robustness Index-II for a 3R-manipulator (Condition-III the first link length taken as 2 unit, second link length as 1.5 unit and third link length as 0.5 unit, the angles are increased with increment of 10°)

Fig. 8 Kinematic model of planar 4R serial manipulator



$$T^{-1} = \begin{bmatrix} \frac{1}{r_1} & 0 & 0 & 0 \\ t_{21} & \frac{1}{r_2} & 0 & 0 \\ r_1 & r_2 & & \\ t_{31} & t_{32} & \frac{1}{r_3} & 0 \\ r_1 & r_2 & r_3 & \\ t_{41} & t_{42} & t_{43} & \frac{1}{r_4} \\ r_1 & r_2 & r_3 & r_4 \end{bmatrix}$$

$$J_a = J_q T^{-1} \text{ (or) } J_q = J_a T$$

6 Results of 4R Manipulator

The performance indices are evaluated for the 4R planar serial manipulator with three different sets of lengths, and the results are given below. The changes in the link lengths of serial manipulator affect the performance and stiffness capabilities of the manipulator (Figs. 9, 10, 11, 12, 13 and 14).

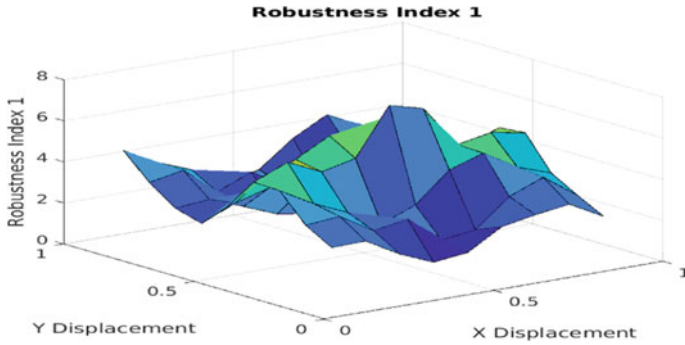


Fig. 9 Variation of Robustness Index-I for a 4R-manipulator (Condition-I the first link length taken as 1 unit, second link length as 1 unit, third link length as 1 unit and fourth link length taken as 1 unit, the angles are increased with increment of 10°)

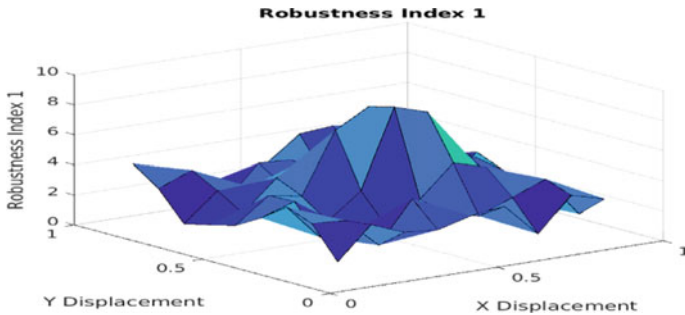


Fig. 10 Variation of Robustness Index-I for a 4R-manipulator (Condition-I the first link length taken as 1 unit, second link length as 1 unit, third link length as 1 unit and fourth link length taken as 1 unit, the angles are increased with increment of 10°)

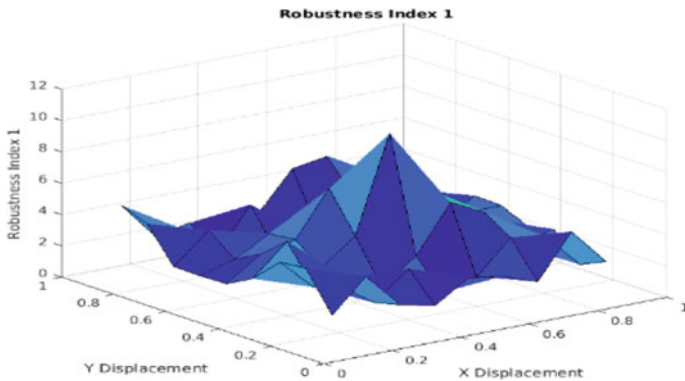


Fig. 11 Variation of Robustness Index-I for a 4R-manipulator (Condition-I the first link length taken as 1 unit, second link length as 1 unit, third link length as 1 unit and fourth link length taken as 1 unit, the angles are increased with increment of 10°)

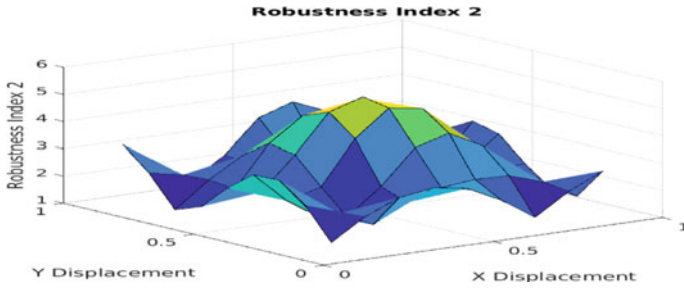


Fig. 12 Variation of Robustness Index-I for a 4R-manipulator (Condition-I the first link length taken as 1 unit, second link length as 1 unit, third link length as 1 unit and fourth link length taken as 1 unit, the angles are increased with increment of 10°)

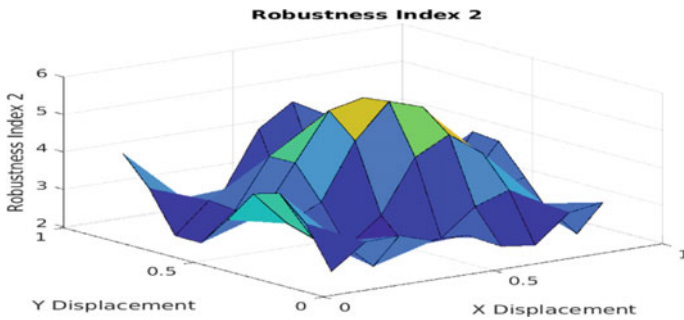


Fig. 13 Variation of Robustness Index-I for a 4R-manipulator (Condition-I the first link length taken as 1 unit, second link length as 1 unit, third link length as 1 unit and fourth link length taken as 1 unit, the angles are increased with increment of 10°)

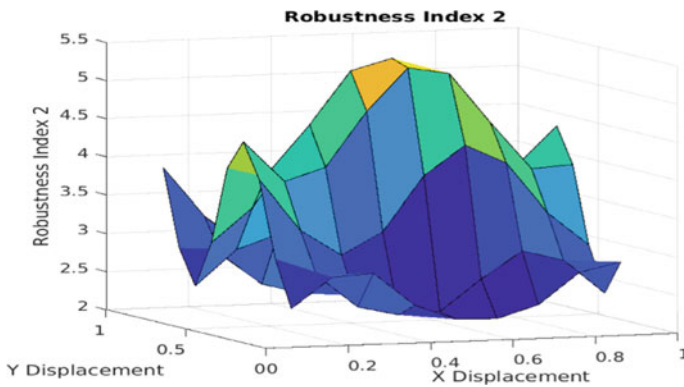


Fig. 14 Variation of Robustness Index-I for a 4R-manipulator (Condition-I the first link length taken as 1 unit, second link length as 1 unit, third link length as 1 unit and fourth link length taken as 1 unit, the angles are increased with increment of 10°)

7 Conclusions

Most of industrial robot manipulators have actuators installed away from the joint they have control and have driven mechanisms connecting actuated joints. For such robots, the joint variables are not equal to the actuator variables. First all the possible actuator-based structures are identified for the planar serial 3R, 4R manipulators. The 3R and 4R manipulators are mathematically modeled, and the performance of the manipulator in terms of Robustness Index is presented in the paper. The maximum values of RI-I values of 4R manipulator are observed in the case-I, II and III as follows 8.83 (0.5, 0.4), 7.54 (0.5, 0.4) and 7.68 (0.5, 0.5). The maximum values of RI-II values of 4R manipulator are observed in the case-I, II and III as follows 5.17 (0.5, 0.4), 5.74 (0.5, 0.4) and 5.4 (0.5, 0.5). The maximum RI-I values of 3R manipulator are observed in the case-I, II and III as follows 30.8622 (0.5, 0.2), 30.41.9 (0.8, 0.2) and 32.82 (0.8, 0.2). The maximum values of RI-II values of 3R manipulator are observed in the case-I, II and III as follows 3.75, 5.67, 4.30 all these maximum values are found at (0.5, 0.5) in the workspace, from these results can conclude that the best location to place end effort or manipulated object in case of 3R manipulator and 4R manipulator is the center of the total workspace.

References

1. Sciascia A, Cromwell R (2012) Kinetic chain rehabilitation: a theoretical framework. *Rehabil Res Pract* 2012, Article ID 853037, 9. <https://doi.org/10.1155/2012/853037>
2. Rojas N, Thomas F (2013) The univariate closure conditions of all fully-parallel planar robots derived from a single polynomial. *IEEE Trans Rob* 29:758–765. <https://doi.org/10.1109/TRO.2013.2242376>
3. Smys S et al (eds) Computer networks and inventive communication technologies. Lecture notes on data engineering and communications technologies—investigation of the static and dynamic path planning of mobile and aerial robots. https://doi.org/10.1007/978-981-15-9647-6_82
4. Chiaverini S, Oriolo G, Walker ID (2008) Kinematically redundant manipulators. In: Siciliano B, Khatib O (eds) Springer handbook of robotics. Springer, Berlin. https://doi.org/10.1007/978-3-540-30301-5_12
5. Ernesto Solanes J, Muñoz-Benavent P, Armesto L, Gracia L, Tornero J (2021) Generalization of reference filtering control strategy for 2D/3D visual feedback control of industrial robot manipulators. *Int J ComputIntegr Manuf*. <https://doi.org/10.1080/0951192X.2021.1973108>
6. https://beckassets.blob.core.windows.net/product/readingsample/784301/9780387095370_e_xcerpt_001.pdf
7. Saheb SH, Babu GS (2020) Modeling and evaluation of performance characteristics of redundant parallel planar manipulator. Lecture notes on data engineering and communications technologies, vol 46. Springer, Cham. https://doi.org/10.1007/978-3-030-38040-3_27
8. Klimchik A, Magid E, Caro S, Waiyakan K, Pashkevich A (2016) Stiffness of serial and quasi-serial manipulators: comparison analysis. In: 2016 International conference on mechanical, system and control engineering (ICMSC 2016), May 2016, Moscow, Russia. fihal-02947183f
9. Klimchik A, Pashkevich A (2017) Serial vs. quasi-serial manipulators: comparison analysis of elasto-static behaviors. *Mech Mach Theory* 107. <https://doi.org/10.1016/j.mechmachtheory.2016.09.019>

10. Singh D, Choudhury R, Singh Y et al (2021) Workspace analysis of 3-DOF U-shape base planar parallel robotic motion stage using shape memory alloy restoration technique (SMART) linear actuators. *SN Appl Sci* 3:511. <https://doi.org/10.1007/s42452-021-04490-y>
11. Zhang DS, Xu YD, Yao JT et al (2018) Analysis and optimization of a spatial parallel mechanism for a new 5-DOF hybrid serial-parallel manipulator. *Chin J Mech Eng* 31:54. <https://doi.org/10.1186/s10033-018-0251-4>
12. Al-Widyan K, Angeles J (2003) Recent advances in integrated design and manufacturing in mechanical engineering. Kluwer Academic Publisher, New York
13. Angeles J (2005) An innovative drive for wheeled mobile robots. *IEEE/ASME Trans Mechatron* 10(1):43–49. <https://doi.org/10.1109/TMECH.2004.842231>
14. Ting KL, Long Y (1996) Performance quality and tolerance sensitivity of mechanisms. *ASME J Mech Des* 118:144–150
15. Zhu J, Ting KL (2001) Performance distribution analysis and robust design. *Trans ASME J Mech Des* 123

Deterioration of Daily Life in COVID-19



Shubhangi V. Urkude and D. Saravanan

Abstract COVID-19 pandemic has affected the normal life of all the human beings in the whole world. It exaggerated all the sectors in the business domain and the daily needs of people. In this paper, we are going to discuss the impingement of pandemic outbreak on different business sectors and day-to-day life of human being. To study the influence of pandemic, a survey is conducted for the peoples of different age groups, gender and different occupation across India. The responses are analyzed, which shows only 5% of the businesses are in profit; these include grocery, health care, etc. Majority of the businesses such as tourism and daily needs were not affected. Regarding the job status, most of the employees working in the private sector were getting insufficient salaries and some of them lost their jobs also. This pandemic adversely affected both the personal and professional life of human being. The collected data is analyzed using various visualization charts and tables.

Keywords COVID-19 · Pandemic · Business domains · Visualization · Outbreak

1 Introduction

COVID-19 is a pandemic which spread rapidly in the globe. The distribution of infection is more for virus and bacteria due to that the disease spread rapidly in the whole world. Such pandemic causes huge damage and dispersed easily from person to person. Now, the entire humanity is experiencing the same, and COVID-19 is the longest pandemic ever happened in the history. COVID-19 or SARS-Co-V-2 belongs to a family of single-stranded ribonucleic acid (RNA) viruses known as coronaviridae (biological name for coronavirus). Basically, this virus is affecting mammals such

S. V. Urkude (✉) · D. Saravanan

Department of Operations and IT, ICFAI Business School (IBS), Hyderabad, The ICFAI Foundation for Higher Education (IFHE) (Deemed to be University u/s 3 of the UGC Act 1956), Hyderabad, India
e-mail: shubhangini@ibsindia.org

D. Saravanan
e-mail: devarajsaravanan@ibsindia.org

as birds and reptiles. Paules et al. [1] told that COVID-19 causes mild infections such as common cold and respirational region infection up to 10–30% in case of adults. As the review done by US Centers for Disease Control and Prevention, the symptoms may appear after, 2–14 days of exposure to affected person. During that period, necessary precautions such as self-quarantine, hand sanitization and wearing mask should be taken by the affected person to prevent spreading of virus. Initially, the virus was found in Wuhan, China local food market, latter dispersed in the whole world. Many researchers studied about the coronavirus, but till now, exact origin was unknown. Some conclusion has been made that mammals such as bats are highly affected by this virus.

Banerjee et al. [2] stated that bat was the main cause of spreading many viruses including coronaviruses (CoVs), and also, it was migrated to humans as well as other agricultural animals. There is proliferation of such virus as more human exposes to the wild animals. The spread of virus has vigorously affected the human life. Increasing number of recognized cases, including the healthcare professionals, shows that explosion of SARS-CoV-2 is more. The number of confirmed cases increased to 185 million as on 09th July 2021. Nationwide lockdown was announced by the various countries including India, to reduce the spread of coronavirus. Due to complete lockdown, various businesses and the human life are affected throughout the country. Professionally and personally, every human being got affected including business, service, house-women, students and others.

This paper is organized as follows: The literature survey is discussed in Sect. 2. Data collection and preprocessing are discussed in Sect. 3 followed by result and discussion in Sect. 4. The conclusion and future scope are elaborated in Sect. 5.

2 Literature Survey

Tsui et al. [3] discussed about importance of anticipating and spreading of infectious disease in the community. They proposed a solution using artificial intelligence and simulation methods to improve the global health. They proposed subset sampling algorithm for heterogeneous data collection, and it was tested on 2–3 million populations in Taiwan. As mentioned in the global report on food crises, there is a shortage of food supply due to lockdown in the entire country. The supply demand chain is unbalance because of the lack of transport availability and nutrition level was gone down. The main reason for food crises was movement of supplies and staffs. In the agricultural sector, local mobility was reduced and food insecurity poverty level was increased. Many migrants are at high risk of no protection, insecurity of food and exploitation. This pandemic also impacted on food production as 80% of the population in India rely on the agriculture products. Due to lack of transport facility for agricultural products, supply was reduced between cities and towns. Reduction in supply leads to increase in cost and poor people lost their employment. COVID-19 pandemic severely affected the social and political peace among the people [4]. Like

this, there were many pandemics affected the whole world and that are discussed below.

Influenza is frequently called as “the flu,” a communicable disease, which occurs due to an influenza virus. This outbreak lasts for a year from 1847 to 1848 and has symptoms such as high temperature, throat pain, cold, arthritis, headache, cough and tiredness. Duration of this flu was nearly 2–7 days, and the symptoms will be seen after one to four days of exposure to affected person. The precautionary measures should be taken such as washing hands regularly, take influenza vaccine and use surgical masks. Webby and Webster [5] discussed about the pandemic and gave an answer to “Are we ready for pandemic Influenza?,” whether we can fight against Influenza or not.

Bubonic plague was type of plague caused by bacterium *Yersinia pestis*. When the infected flea, *Xenopsylla cheopis* (the rat flea) bite anyone, it will spread to that thing. The whole world was suffered for around 105 years from 1855 to 1960. Generally, it has symptoms such as mild illness, headaches, stomach upset and swelling on the lymph nodes. Its symptoms will be visible after coming into the contact of affected person within one to seven days. Antibodies like streptomycin, gentamicin, or doxycycline are the only ways to stay safe from the virus. Zietz and Dunkelberg [6] stated the history of plague and the research on the causative agent *Y. pestis*.

Encephalitis lethargica was mostly know as variant of encephalitis. It was frequently known as “sleeping sickness” or “sleepy sickness” (distinct from the tsetse fly). Von Economo, a neurologist and the Jean-Rene Cruchet, the pathologist, explored this disease in 1917. This is very dangerous disease, and it will attack the brain, which makes the affected person unconscious. The outbreak lasts for 11 years, from 1915 to 1926 and has symptoms such as high temperature, throat pain, unconsciousness, sleep inversion, headache, double vision, tiredness and catatonia. Specific symptoms were treated with immune modulating therapies and dramatic symptoms were treated with Levodopa (L-DOPA) and another anti-Parkinson drug. McCall et al. [7] discussed about Encephalitis lethargic and the connections exist between encephalitis lethargica and influenza.

In 1918, another pandemic exists that is known as flu pandemic and it was due to the Spanish flu. It was produced by H1N1 influenza virus. The world suffers for two years due to the outbreak of pandemic from 1918 to 1920. It has symptoms such as throat pain, headaches and mild fever in the first wave. Ekici et al. [8] developed monitoring system to find food requirements of different geographical areas called as dynamic update approach. This model was tested in Georgia State and used successfully for one year to provide the sufficient food to infected people. They also discussed about all the influenza pandemics and state the cause of various influenza pandemics like Spanish flu and Asian flu.

The psittacosis pandemic was there for one year from 1929 to 1930 and often called as great parrot fever pandemic. This eruption of parrot fever occurred continuously for one year. Basically, it was increased due to movements of birds and breeding in the packed containers for selling. It was originated from parrots of South America. Telfer et al. [9] discussed about the psittacosis outbreak and its cause. In 1957–1930, another pandemic arises that is known as Asian flu which due to influenza virus.

This was a worldwide, and it was caused by H2N2, one of the variants of H1N1. It was first found in Guizhou, China, and due to that, millions of people were affected throughout the world.

The cholera pandemic was one of the major pandemics, and it was happened in 1961–1975. The variant of this exists till now in the world. Depending on the type of this strain, it is known as E1 Tor. This initially found in Indonesia in the year 1961 and later migrated to Bangladesh in 1963. It also reached India in 1964 and found in Soviet Union during 1966. Gradually, it spread to Odessa in July 1970 and 1972 in Baku, but Soviet Union did not reveal this information to outside world. It spread in North Africa, Japan and the South Pacific by mid of 1970s. The Hong Kong flu started in 1968 for a year. This flu pandemic destroyed nearly four million population in the globe. It occurs due to H3N2 strain which is a descended of H2N2. It created from the genetic process, in which multiple genes are rearranged to form new variant. WHO research stated the symptoms, history and cause of the pandemic. Kilbourne et al. [10] discussed about the pandemic, its history, cause and symptoms.

Some of the researchers treated HIV/AIDS or human immunodeficiency virus, as global pandemic and same is announce by WHO recently. This pandemic produces heterogeneous impact in various countries, some regions are badly affected and in some regions impact is less. Giamberardino et al. [11] discussed the impact of pandemic, preventive measures and early analysis of HIV/AIDS. In 2002–2004, SARS produced by severe acute respiratory syndrome coronavirus (SARS-CoV or SARS-CoV-1) is treated as a global pandemic. This eruption was first found in various countries such as Foshan, Guangdong, China, on November 16, 2002. Paolo told about the effect of daily human behavior due to SARS. In Mumps, outbreaks occurred in the twenty-first century and present till today. This viral disease continues to cause outbreaks across the world.

WHO research states about mumps and mumps vaccine in brief? Middle East Respiratory Syndrome (MERS) was new variant of coronavirus due to this many people in several countries were affected. It was first found in Saudi Arabia in April 2012. It has mild symptoms like corona and little cold. Alpha and beta generation variant of MERS can infect humans. MERS-CoV and SRAS-CoV are beta generation coronaviruses. Ramadan and Shaib [12] discussed about the Middle East respiratory syndrome infection and control briefly. They developed an approach for preventing the spread of disease.

The COVID-19 is a global pandemic of coronavirus disease. It is produced by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). It was first found in 2019 December, Wuhan, China. On January 30, 2020, it was declared as public health emergency by WHO and as a pandemic on March 11, 2020. Coughing, sneezing and talking are the primary ways of distributing the virus. The small droplets created by nose and mouth during sneezing and talking distribute the virus to the others. It has most mutual symptoms like fever, tiredness, breathlessness, fatigue and no sensation of smell and taste. Sometimes, it leads to pneumonia and breathing problem. Table 1 shows the summary of all the pandemics which affected the world till now. Chamola et al. [13] discussed about COVID-19 and its impacts on the world and the global

Table 1 Summary of pandemics

Disease name	Time period	Cause of disease	Death cases (total)
Influenza	1847–1848	Influenza virus	Unknown
3rd Plague pandemic	1855–1960	<i>Yersinia pestis</i>	12 million+ including India and China
Encephalitis lethargica	1915–1926	Unknown	1.5 million
Spanish flu	1918–1920	H1N1 virus	17–100 million
Psittacosis pandemic	1929–1930	Linked to parrots from Buenos Aires	1 million
Asian flu	1957–1958	Avian H2N2 influenza	1–4 million
Seventh cholera	1961–1975	<i>Vibrio cholera</i>	Unknown
Hong Kong flu	1968–1970	Influenza A (H3N2) virus	1–4 million
HIV/AIDS	1981–present	Human immunodeficiency virus	32 million+ (23.6–43.8 million)
SARS-CoV	2002–2004	Animal virus	772 K
Mumps	2009	Paramyxo virus	Unknown
MERS-CoV	2012–present	Middle East respiratory syndrome coronavirus	2574 (as of May 2021)
COVID-19	2019–present	Animal virus	185 million (as per 9th July 2021)

economy. They also discussed use of different technologies such as blockchain, IoT, artificial intelligence and so on.

3 Data Collection and Preprocessing

To perform this analysis, survey was conducted among the peoples of various age group, gender and different occupation. Data was collected randomly by the questioner created which includes following questions. Responses were collected using Google form.

- Which age group do you fall under?
- Gender
- State
- City
- Professional status
- Current status of your business
- Business domain
- Job status
- Job sector or domain
- How much COVID-19 affected your professional life? (Rate out of 5)

- How much COVID-19 affected your personal life? (Rate out of 5)
- What will you appreciate about COVID-19?
- Any other issue that you faced because of COVID-19?
- In your opinion what can reduce the effect of this virus? (Till the time vaccine isn't available)

Data consists of total 250 responses. The collected data has some blank entries which were removed as part of preprocessing and cleaning. Depending on the occupation such as service or business form was redirected to collect relevant information. The response collected is having both the qualitative and quantitative data. Quantitative response is in the range of 1–5. 1 indicates less affected, 5 indicate more affected and 3 are considered as neutral.

4 Result and Discussion

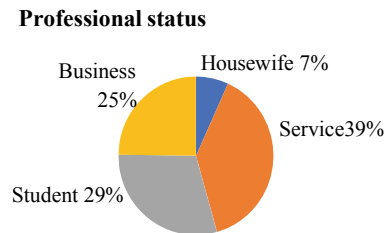
Visual modeling is one of the important techniques to represent the data. Here, we used various visualization charts to show the influence of COVID-19 on the businesses and daily lives.

Figure 1a represents the table for categories of professional status. The total 250 samples are divided into four categories as housewife, student, service and business. The count of each category is also shown in the table. Figure 1b represents the chart for professional status of the collected data in percentages out of 250 samples, in which 7% people are housewives, 25% are doing business, 29% are students and 39% people are in service. Figure 2a represents the service sectors. These sectors are divided into four different categories as first category is education having 15% and lowest among all the categories. Second category is the sector having 21%, third

Fig. 1 a Professional status sample count. b Professional status ratio

Professional status	Count
House wife	17
Service	97
Student	74
Business	62

(a)



(b)

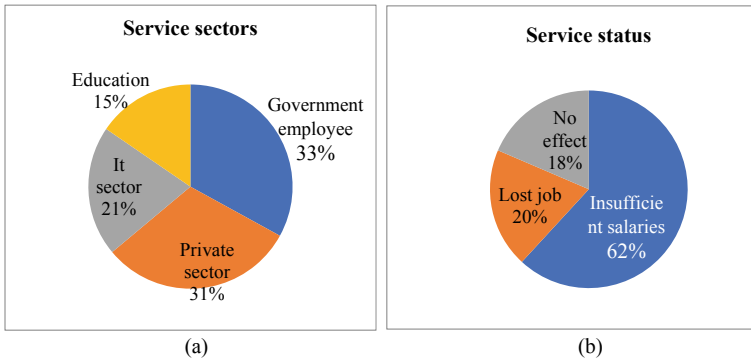


Fig. 2 a Service sectors. b Service status

category is government employee having 33% count which include jobs like police, railway, banking sector, etc. and it is the highest count and fourth one is the private sector containing 31% out of 97 samples for the service sector. Figure 2b shows the service status. In 39% of total samples in the service domain, 20% of the people lost their jobs which includes hotel waiter, people working in cinema theaters, etc., 62% people are getting insufficient salary and 18% of the people have no effect on their service status. The unemployment is increased due to loss of jobs, so they are not in position to fulfill their daily needs. This leads to the elevation of crime rates in the society and also severely affected the economic conditions in India.

Figure 3a represents the business status of all the businesses collected in the sample data. The data is having 62 distinct samples in which 26% of the businesses are running without any effect. This includes tourism, health care and daily needs which are the essential things for human beings. 5% of the businesses are running in profit which includes grocery shops, and 69% businesses are running in loss. The other businesses like cloths, automobiles, electronics and other small businesses are in the loss because these are not the essential things for the human life. At some

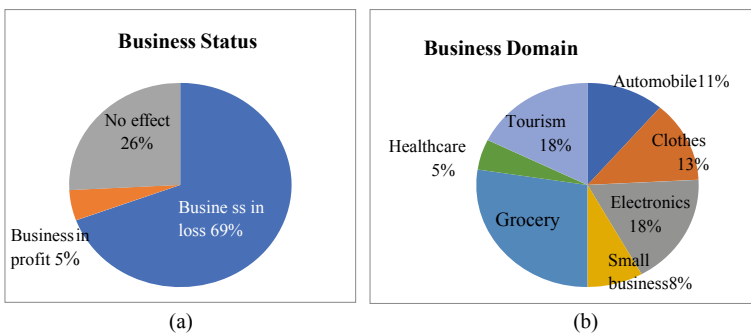


Fig. 3 a Business status. b Business domain

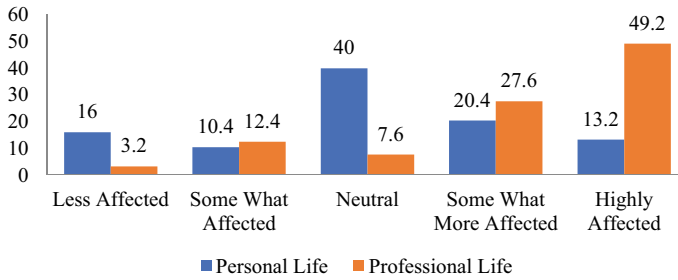


Fig. 4 Personal and professional life in COVID-19

places in rural areas, grocery and healthcare business also running in loss because people are not having sufficient financial support to buy required things. Fig. 3b represents the various business domains in which grocery is the highest and health care is the least count. Figure shows automobile is having 11%, cloths having 13%, electronics having 18%, small businesses are 8%, grocery having 27%, health care having 5% and tourism having 18%.

Figure 4 represents the chart for personal and professional life in COVID-19. In this figure, x-axis represents the ratings given between 1 and 5 on personal and professional life, and y-axis represents the count for each rating. For the personal and professional life, quantitative data is collected at the scale of 5.

In the range 1 is less affected, 2 is somewhat affected, 3 is neutral, 4 is somewhat more affected and 5 is highly affected people in the personal and professional life. According to the figure, 49.2% of the people are highly affected in professional life that means many have lost their jobs, those are doing job are not getting proper salary and so on. 40 and 7.6% are having the neutral opinion about effect of COVID-19 in personal and professional life, respectively. As per the analysis, the people are highly affected in professional life as compare to the personal life.

Different people in the various age group have variety of opinion about what will you appreciate about COVID-19? The age group of 0–17 years is saying no study, they got time to spend with family and government came into action and so on. The age group between 18 and 35 says pollution is reduced, they got free time, work from home, online learning is promoted, and people are more concern about their health and so on. Majority of the samples are belonging to this age group. The age group between 36 and 58 is more concern about financial matters. Some are saying life of poor people is spoiled, some are saying they got time to learn new courses and developed new skills, etc. The age group between 59 and 70 also having similar opinion and the age group above 70 is saying good to stay at home and take care of your health.

5 Conclusions and Future Scope

In this paper, impact of COVID-19 on daily life of a common man is discussed. Along with personal and professional life, this also affected the businesses, services and other things. According to the analysis done, personal life was affected more than the professional life. Many people had lost their job, and those were continuing the jobs were getting insufficient salaries. The businesses such as grocery, tourism and health care were running in profit. Other businesses like vegetables, milks and daily needs are running without any effect. It is found that business class wanted the stability of their business back in the market. The service class wanted their full salaries and other benefits; those who lost their way of income are fighting for new jobs. Per day wagers are suffering more because they do not have neither incomes nor way of living and rest all others are facing issues too.

Many good things were happened due to complete shutdown in metropolitan cities like closing the public places, cutting down the transport and work from home. People were getting family time, pollution is reduced to some extent, environment healing was happened, public places were sanitized frequently, peoples tried to look after their health, etc. In future, we can extend this work to collect more data and use machine learning algorithms to predict the future impact of such pandemics.

References

1. Paules CI, Marston HD, Fauci AS (2020) Coronavirus infections—more than just the common cold. *JAMA Network* 323(8):707–708
2. Banerjee A, Kulcsar K, Misra V, Frieman M, Mossman K (2019) Viruses. In: *Viruses and bats*, vol 11, issue 1, p 41
3. Tsui K-L, Wong ZS-Y, Goldsman D, Edesess M (2020) Tracking infectious disease spread for global pandemic containment. *IEEE Intell Syst* 28(6):60–64
4. Food crises in India due to pandemic, pp 1–5, Apr 2020
5. Webby RI, Webster RG (2003) Are we ready for pandemic influenza? *Science* 302(1):1519–1522
6. Zietz BP, Dunkelberg H (2003) The history of the plague and the research on the causative agent *Yersinia pestis*. *Int J Hyg Environ Health* 207(2):165–178
7. McCall S, Vilensky JA, Gilman S, Taubenberger JK (2008) The relationship between encephalitis lethargica and influenza: a critical analysis. *J Neuroviral* 14(3):177–185
8. Ekici A, Keskinocak P, Swann JL (2008) Pandemic influenza responses. In: *Winter simulation conference*, Dec 2008. *IEEE Xplore*, pp 1592–1600
9. Telfer BL, Moberley SA, Hort KP, Branley JM, Dwyer DE, Muscatello DJ, Correll PK, England J, McAnulty JM (2005) Probable psittacosis outbreak linked to wild birds. *Emerg Infect Dis* 11(3):391–397
10. Kilbourne ED (2006) Influenza pandemic of 20th century. *Emerg Infect Dis* 12(1):9–14
11. Di Giamberardino P, Compagnucci L, De Giorgi C, Iacoviello D (2017) Modelling the effect of prevention and early diagnosis on HIV/AIDS infection diffusion. *IEEE Trans Syst Man Cybern Syst* 49(10):2119–2130
12. Ramadan N, Shaib H (2019) Middle East respiratory syndrome. *Germes* 9(1):35–42
13. Chamola V, Hassija V, Gupta V, Guizani M (2020) A comprehensive review of COVID-19 pandemic and the role of IoT, drones, AI, blockchain and 5G in managing its impact. *IEEE Access* 8(1):90226–90265

A Design Model of Copyright Protection System Based on Distributed Ledger Technology



K. Varaprasada Rao and Sandeep Kumar Panda

Abstract Nowadays, to protect and secure interest of innovators and research information in decentralized ledger-based echo system using blockchain technology to minimize the challenges and risks faced by conventional copyright system called intellectual property systems, the authors proposed a model using programmable contracts that ensures to extract the features provenance for tracing of ownership, transfer histories which in turns ensures system transparency and traceability. This paper covers basic understanding of blockchain, existing copyright system, and a new echo system can be implemented using blockchain technology effectively. A solution model is designed for the system along with the explanation of the procedure to build the system.

Keywords Blockchain · Smart contracts · Transparency · Traceability · Decentralized

1 Introduction

In the stream of digital technologies, blockchain is the latest among them. With its unique features, distributed, decentralized, immutability, transparency, and traceability, blockchain is expected to revolutionize the world. In 1991, a group of analysts illustrated this technique to timestamp digital documents to eliminate the possibility of tampering with them. However, in 2009, Nakamoto adapted this technique to create the digital cryptocurrency bitcoin [1, 2]. Distributed ledger technologies (DLT) are used by bitcoin to keep the track of supply and flow of various virtual tokens of financial resources in a distributed and decentralized manner which means no third-party involvement is encouraged in the transactions on bitcoin blockchain.

K. Varaprasada Rao (✉) · S. K. Panda
Department of Computer Science and Engineering, Faculty Science and Technology, ICFAI
Foundation for Higher Education, Hyderabad, Telangana, India
e-mail: varaprasad.fst@ifheindia.org

S. K. Panda
e-mail: sandeepanda@ifheindia.org

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023
S. C. Satapathy et al. (eds.), *Computer Communication, Networking and IoT*,
Lecture Notes in Networks and Systems 459,
https://doi.org/10.1007/978-981-19-1976-3_17

127

Although bitcoin is restricted to the exchange of financial resources, its underlying technology, blockchain, can be utilized in many sectors to solve real-life problems. Blockchain has already played its crucial role in medical, financial, sales, and other sectors. Blockchain is a decentralized distributed ledger built on top of peer-to-peer networks [1, 3] with immutable [4] records in which multiple peers can be part of the network, and they can trade resources or assets robustly from all over the world [5–9]. A replica of the blockchain is distributed to every peer called nodes, across the network. Therefore, if one node crashes, information can be gathered from another node as every node has a replica of the blockchain thus making it immutable.

As a result of the superiority and elevated security, privacy, and trust provided by the blockchain technology, different platforms emerged for the development of applications based on blockchain. These newly emerged platforms include Ethereum [6, 8], R3 Corda [10], IBM Bluemix [11], Hyperledger-fabric [12], Quorum [13], Ripple [14, 15], etc. The most popular and widely used platform for the development of decentralized applications (Dapps) is Ethereum. In this paper, the proposed model is based on Ethereum blockchain, and the objective problem is solved with the help of Ethereum blockchain.

Copyright is a form of intellectual property just like a trademark, patents, and designs. Copyright protects the original work of an author or the creator of the work. So generally, copyright is protected under various forms, i.e., copyright can be filed or protected under literary, artistic, musical, cinematographic, dramatic, and sound recording. The literary work refers to the original work that has anything to do with written content, for example, books, poems, magazines, novels, etc. Artistic copyright refers to anything that has an artistic feature to it, for example, paintings, photographs, sculptures, etc. Cinematographic work includes any audio-visual video recording, for example, films, movies, and all other video recordings [16–19]. Copyright guarantees certain protective measures for the rights of creators over their innovations or creations, thereby safeguarding and merit creativity. Creativity being the foundation of growth, no educated community can afford to neglect the fundamental necessity of supporting the same. Creativity is the key to the social and economic development of a society. A favorable environment is created for creativity because of the security granted by the copyright to the works of writers, dramatists, architects, artists, and producers of cinematograph films, etc. which inspires them to create more and persuade others to create.

The content digitalization has substantially increased the probability to replicate and distribute information. Content copying with no loss in quality at a very low cost can be achieved with ease in the era of digitalization, whereas access and distribution of information are accelerated and increased by the internet. Furthermore, different ways or features for sharing knowledge and information are universally available in this age of electronics. However, the ability to perfectly copy and distribute the digital content with ease facilitates plagiarism, illegal distribution, misuse, and misappropriation thereby, posing a threat for the original creators or producers of the content or information as it becomes increasingly problematic to sell the content for a fruitful price. Furthermore, copyright infringement [20, 21], forged documents are the main problems associated with the existing copyright system. Copyright infringement

means the usage of copyright-protected works without the permission of the creator, thereby violating certain unique rights provided to the copyright holder, for instance, the right to distribute, reproduce, and display the protected work.

However, copyright law [22–24] does not really serve their deliberate purpose of helping the public. The laws are so excessively broad that they suppress an individual's creativity rather than encouraging it. Many people use others created or copyrighted work to produce new innovative works such as remix etc. The legality of these remixes depends on its qualification for fair use. Therefore, the risk and unpredictability of being sued for copyright infringement prevent people from creating innovative works. Furthermore, these laws being so complex and uncertain that they can be effortlessly exploited by companies with access to lawyers, making it expensive and too complicated for independent artists to enforce the rights provided by the law. Fair use of the content is the main defense for copyright infringement. The court trials are expensive which gives large companies the advantage over the infringer resulting in a stop of his/her use even if it may be legal.

2 Literature Survey

Blockchains are incredibly popular nowadays, and the above-discussed problems can be solved with the help of blockchain technology. Blockchain adds a layer to the internet ensuring trust among people by enabling assured trusted records. The trust is established by the computer code of the technology instead of individuals and centralized organizations. In this respect, blockchain can be recognized as a trust machine in its ability to empower a network where trust is made by design, it is incorporated with the framework consequently in light of the fact that the blockchain makes a trusted distributed database. Blockchain can function as a ledger that may act as a record for the storage of transactions and value. Since olden times, ledgers have been the foundation of our economy to log transactions and payments for the purchase and distribution of commodities or the trade of properties such as land [25–28]. The evolution of banking, the development of currencies, commerce, and loaning were empowered by these ledgers. In recent decades, digital computers are being used to maintain accounts thus reducing the possibility of human error and revolutionizing the accounting system. In the present day, distributed ledger technologies are revolutionizing the accounting system by maintaining accounts over an international network of computers which is decentralized and cryptographically secure [29]. Blockchain is a distributed decentralized ledger technology on which all the information can be stored on the ledger safely and precisely using cryptographic encryption [30–32]. The information stored on these ledgers can be obtained by using cryptographic signatures and the public, private keys. Any alterations or extensions made to the record are reflected and replicated to all nodes in a matter of seconds or minutes. Every node connected to the network has the replica of the blockchain and can access any information shared across the network. Moreover, with the provenance feature of blockchain, the history of the information can be traced back to the origin of

the information ensuring the authenticity of the information. These ledgers could be used for logging, managing, tracking and transacting of all types of properties. As we know, every asset can be registered, stored, and exchanged on the blockchain network; therefore, every asset or property registered on the blockchain could become smart property. Every asset stored on the blockchain is encoded with a unique differentiator which can further be used to track, manage, and exchange assets on the blockchain network. For instance, the copyright protection system could use distributed ledgers such as blockchain to register and store any type of digital assets and provide them with a unique identifier in terms of hash values. Therefore, after decades of research, blockchain can be acknowledged as a disruptive technology that could revolutionize the world.

In the era of disruptive technologies, research and development in the field of copyright protection play an important role in providing copyright holders with solutions to fight copyright infringement. A lot of discussion and research has been done to combine blockchain technology with copyright protection problems to ensure the elimination of copyright infringement [33–37].

The most significant key features for the advancement of blockchain technology are immutability and transparency. Immutability is linked to the fact that once a data is uploaded on the blockchain network; it cannot be altered making the record tamper-proof. Furthermore, transparency ensures visibility and inspection of blockchain so that unauthorized transactions cannot be carried out. Distinct solutions have been provided to deal with the problem of copyright infringement, for instance, [38–43] restricting the use of copyright work by inlaying digital watermarks together with identification information in the content. Images with a digital watermark are stored in the blockchain, and timestamp authentication is provided for multiple copyrights. IPFS is used to store and distribute watermark images. References [44–47] proposed a basic intellectual property protection model based on blockchain technology. Users can upload their created content on the platform. The uploaded content can be a video, scripts, literary work, etc., and when the public clicks to view the content or watch the video, the smart contract enables the platform to carry out automatic fee payment to the copyright holder and the distributor of the work. However, this model does not carry out ownership transfer of the digital content or copyright work. Our design solves the issue of ownership transfer and also traces the content ownerships with the provenance feature of blockchain, thus achieving transparency and traceability [48, 49].

3 Proposed Model

In this section, we propose a solution model for copyright protection to reduce time delays and frauds, to eliminate copyright infringement which is recognized by data immutability, decentralization, and traceability of blockchain technology. The proposed copyright protection system involves a large number of users that are linked via a decentralized network. The users or nodes can have the attributes of the

creator, buyer, and seller. For the process of ownership transfer, an event response mechanism is designed to assure that both the parties involved in the transaction concur on the receipt and ownership transfer, and the process will be perpetually stored on the blockchain.

3.1 System Security Requirements

In this paper, the proposed blockchain-based copyright protection solution model should link up with the following security essentials.

Data permanency: To ensure the robustness and reliability of the copyright protection system, the proposed solution should have the feature of immutability so that no one can change or tamper with the data.

System independency or self-reliance: All the nodes on the network should be independently maintaining a trusted environment for exchanging and updating the information thus preventing human interference. Moreover, a fixed and predictable algorithm should be followed for data exchange in the system.

Protection from malicious attacks: Due to the decentralized nature of blockchain, the nodes in the international network system are unfaithful. Therefore, the system should be robust enough to prevent malignant nodes from doing illegal transactions.

3.2 Solution Model Architecture

Phase-1 As shown in Fig. 1, the blockchain-based copyright protection system illustrated in this paper mainly includes the creation of a platform on top of a decentralized blockchain network where users can register using their name, Aadhar number, email ID, and mobile number. Aadhar number is necessary to ensure that a single person does not create multiple accounts. The user registration on the platform is implemented using JavaScript and Nodejs. Any user can have the attributes of the creator, seller, and buyer. The users within the platform or the creators to upload their creative or innovative work such as photographs, lyrics, and scripts on the decentralized distributed network. As the user uploads the content, a zero-knowledge proof mechanism is used to check if the uploaded content already exists on the platform or the blockchain network. However, if the content which the user is trying to upload already exists on the platform, then an error will be thrown, not allowing the user to upload the content on the platform. A cryptographic hash created for each copyright record which contains the file as well as copyright holders name and email will be stored on the blockchain network, thus making the record immutable.

Phase-2 Figure 2 describes the scene after the user registration. After the registration is completed on the platform, users can browse or search for the created work of other users on the platform. Furthermore, if they wish to view the content of the work, they have to request the creator or copyright holder of the work to give access

Copyright Protection

Phase-1

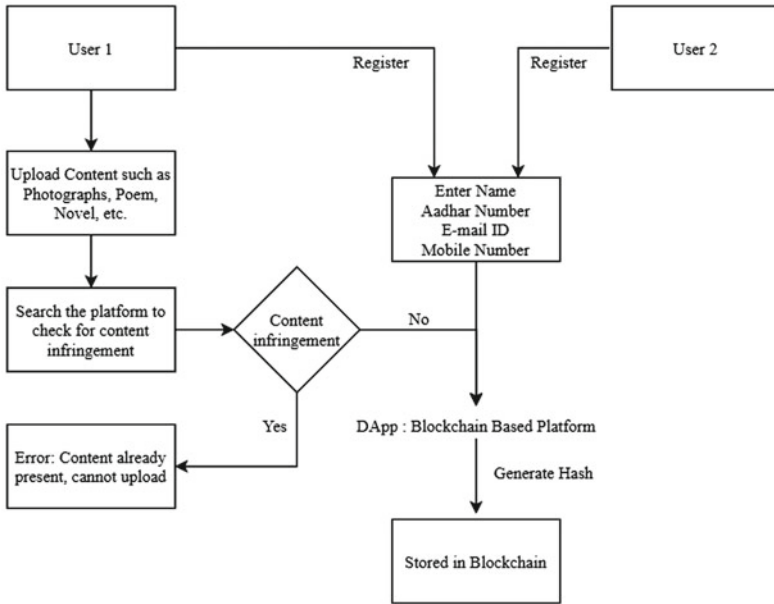


Fig. 1 Copyright registration flow diagram

to view the file or content. This step is taken to eliminate copyright infringement as the user will not be able to directly view or copy the content of the copyright holder and use it somewhere else for his profit. However, even after viewing the content of the file, if someone tries to use it somewhere else, then the copyright holder has the record of the people who viewed his content and can register a case against that person. After viewing the content if the user is interested in purchasing it, they can again request the creator or copyright holder for the purchase of the content. If the copyright holder agrees to sell the created work for a set fee, then the ownership is transferred to the user purchasing the work. However, if the copyright holder does not agree to sell his work, then the buyer has the option to discuss licensing options with the copyright holder, i.e., request the creator to license the work to him for use, for some duration. This transfer of ownership and licensing options is carried out with the help of smart contracts.

View: Requesting the copyright holder for viewing the content is carried out by using JavaScript and Nodejs. The recorded information of the people who viewed the content will be stored on the blockchain.

Purchase: Purchasing of the content or the ownership transfer will be performed using smart contracts. The smart contract will be coded to perform trusted transactions between the buyer and seller. Thus, making purchasing of the work and ownership transfer a matter of minutes.

Copyright Protection

Phase-2

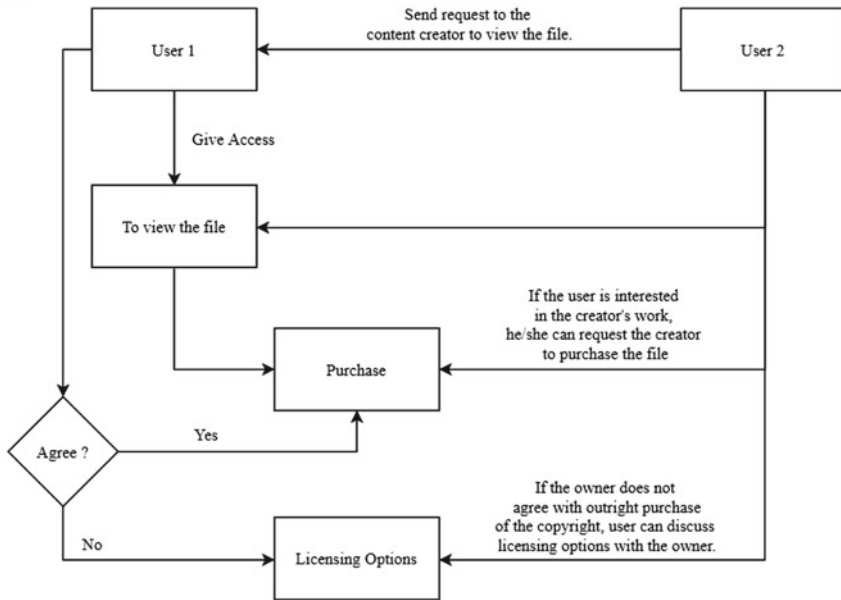


Fig. 2 Copyright purchasing and licensing flow diagram

Licensing options: Agreement for the licensing duration of the content will be carried out using smart contracts. The user will be allowed to use the copyright content for a specific duration for a set fee depending on the duration of the license.

Phase-3 The last phase of the model shown in Fig. 3 describes the process of ownership transfer or licensing of the created work. If the copyright holder as the seller agrees to transfer the copyright ownership to the buyer for a set fee or to license the work to him for some duration for a specific amount of fee, the transactions corresponding to both the parties are validated by nodes across the distributed network and stored on the blockchain network. As the transactions of all the ownership transfers are stored on the blockchain, with the provenance feature, the ownership can be tracked back to the original creator of the content or work. The ownership transfer or licensing of the content will be accomplished by smart contracts.

Validation: Transactions carried out are to be validated by nodes across the distributed network using some consensus mechanism. Currently, the following four mainstream consensus algorithms are widely used in blockchain projects: PoW (Proof of Work) [40], PoS (Proof of Stake) [41], PBFT (Practical Byzantine Fault Tolerance) [42], DPoS (Delegated Proof of Stake) [43]. Proof of work consensus mechanism demands a lot of computational capability making it difficult to preserve its security and stability using the blockchain system [45, 46].

Copyright Protection

Phase-3

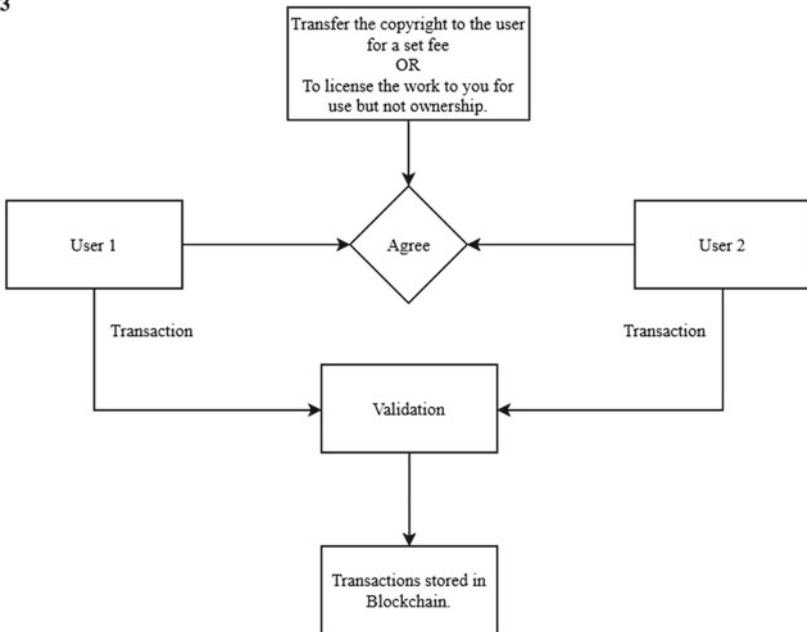


Fig. 3 Transaction flow diagram

3.3 Smart Contract Design

This paper designs two smart contracts, namely content registration contract (CRC) and ownership transfer contract (OTC). The main contract to be deployed on the blockchain network is the CRC contract. Once a CRC contract is deployed, it has a function to deploy the instance of the OTC contract which acts as a key to the linking and cooperation of the two contracts. In the CRC contract, every uploaded content on the platform is assigned a hash value which is stored on the blockchain network. The ownership transfer histories of the copyright content can be queried by the end-user once he gets access to view the details of the content. The right to update the contract status is given to accounts in the endorsement record maintained in each contract. The endorsement records are set of approved users' Ethereum address in the contract. Description of the function of each contract is given below:

(1) **Content Registration Contract (CRC).**

The system manager deploys the CRC contract and a `contentregister ()` function is added, which stores the content information permanently on the blockchain network. The owner of the work registers and uploads the content

on to the platform including content owner name, content title, content description, and the content itself. A `verify()` function modifier is used in `contentregister()` function to check if the registering content is already present on the platform or not. If the content or created work is not present on the platform then the function returns “true” and the content or work is registered on the platform. Otherwise, if the content is present on the platform, then an error is thrown conveying that the content cannot be registered. Only the content title, description, and hash are visible to the users on the platform.

(2) **Ownership Transfer Contract (OTC).**

The OTC contract is deployed by other users on the platform by interacting with the front-end webpages. The CRC contract provides a function that creates a new instance of OTC and stores the resulting address. The OTC contract has two main functions namely `purchase()` and `license()`. Whenever a user clicks on the button events for these functions, the corresponding functions are invoked redirecting the user for purchase or licensing of the content. Furthermore, after the purchasing or licensing of the content, the buyer is provided with an ownership or licensing certificate certifying the ownership of the buyer or the license of the licensee over the content.

The algorithm logic for the three main functions namely `contentregister()`, `purchase()`, and `license()` will be given in the system implementation section.

4 System Implementation

In this section, the implementation of the solution model proposed in this paper is explained. The deployment, testing, and compilation of smart contracts can be carried out effectively using the truffle framework [47]. Truffle is a development platform for Ethereum which can be used to develop, test and deploy smart contracts. It is an all-in-one platform for solidity contracts. The text editor used for the project is Visual Studio Code [48]. Visual Studio Code is an open-source, free, lightweight but powerful text editor that can be set up as a solidity IDE (6.0.1) by installing some extensions or plugins. The front-end framework used here is Web3.js [20, 49] which is a JavaScript library, a portal or window into the Ethereum network with a collection of JavaScript objects allowing us to interact with Ethereum network to transfer money, store data, deploy contracts, etc. Truffle HD wallet provider is used in our implementation allowing us to connect to the Rinkeby test network hosted through infura, unlocking some accounts to use for testing purposes.

The key to making the DApp user-friendly is the interaction with contracts via front-end webpages. The webpages are developed using HTML and CSS code. Furthermore, the connections are established with HTML to interact with the front-end webpage. Interaction with contracts is carried out with button events on the webpage allowing users to call methods, read blockchain data or deploy a contract by clicking button events. For testing purposes, only content registration contract (CRC)

is deployed using the truffle framework. With the front-end interaction on webpages, other contracts can be automatically deployed using button events. Furthermore, for code testing, a local test network is used, Ganache, a local development blockchain used to simulate the blockchain. The ganache is an Ethereum client designed specifically for developers used to deploy and send transactions. It has only one node in the Ethereum network so that we have only one instance of ganache and there is no need to set miners; therefore, all the transactions sent to ganache will be mined instantly, i.e., auto-mined. Furthermore, ganache generates ten addresses that are already unlocked with 100 fake ethers making it overall simpler to test the smart contracts. The ganache runs in local memory, thus swiftly approving transactions, returning execution outcomes in actual time. After the deployment of the smart contract on the Ethereum blockchain, it cannot be modified or tampered. Therefore, it is most favorable to test the smart contract using a test network before deploying it on the main Ethereum network.

However, the view feature which lets the users request the owner of the content for the access to view the content is implemented using JavaScript and Nodejs. Once the access is granted by the owner, the user or buyer can view the full information about the created work such as the registration date, owner's name, purchase cost, and the content itself. The users can also view the ownership histories of the content saved on the blockchain after the access is granted. The recorded information of the people who viewed the content will be stored on the blockchain.

The front-end webpage implementation of the main functions of the system namely register, purchase, and license of the copyrighted work is shown below.

Figure 4 displays the home page for the copyright protection platform. After the user registration, the first page that the user sees on the platform is the home page. All the copyright works are displayed, which users can browse on the home page. A “register copyright” button is shown in Fig. 4, clicking on which the user is directed on the copyright registration page.

Figure 5 displays the copyright registration page of the platform. The users need to fill the registration form with various fields such as work title, creator name, and created work where the user has to upload the content and click on the “register” button to register their copyright. Moreover, the platform checks if the created work already exists or not, if the content does not exist then copyright registration can be performed; otherwise, an error is shown stating the copyright cannot be registered.



Fig. 4 Platform home page

Copyright Protection Sytem Copyrights +

Register a Copyright!

Work Title
Movie Script - Dramatic

Creator Name
John Doe

Created Work
Upload a File

Register!

Fig. 5 Copyright registration page

Figure 6 displays the copyright purchasing page of the platform. The procedure for purchasing copyright is much simpler and user-friendly. The user is redirected to the transaction page after entering the name and clicking the purchase button. A transaction window is popped up asking approval for the transaction, and after the approval, the ownership is transferred to the buyer. Moreover, an ownership certificate is generated for the buyer stating his authority over the copyrighted work.

Figure 7 displays the copyright licensing page of the platform. The user has to fill the license form with licensee name and license duration as fields. As the user clicks on the “get license” button after filling the details, a transaction window is popped up asking approval for the transaction, and after the transaction approval, the licensee is provided with the license of the copyrighted work. A license certificate is generated stating the licensee name, license duration, and authority of the licensee for using the copyrighted work for a specific duration.

Copyright Protection Sytem Copyrights +

Purchase a Copyright!

Buyer Name
Victor Hoffman

Purchase!

Fig. 6 Copyright purchasing page

Copyright Protection Sytem Copyrights +

License a Copyright!

Licensee Name
Alex Dcruz

License Duration
12 Months

Get License!

Fig. 7 Copyright licensing page

The screenshot displays a web interface for a 'Copyright Protection System'. At the top, there is a navigation bar with 'Copyrights' and a '+' icon. Below this, the 'Copyright Details' section is shown. It contains several information cards:

- Address of Owner:** 0x6cdb4D7A630Bb3bf2379c9A0d3C49974d81a58b2. Description: The owner created this copyright.
- Copyright Registration Date:** 20/10/2016. Description: Date on which the copyright was registered.
- Owner Name:** John Doe. Description: Name of the Copyright Owner.
- Purchase Cost:** 200000. Description: Cost associated with purchase of the copyright.
- Licensing Cost Per Month:** 10000. Description: Per month cost for licensing the copyright work.
- Created Work:** Description: The created work will be shown here such as photographs, lyrics, scripts etc.

At the top right of the details section, there are two buttons: 'Purchase Copyright' and 'License Copyright'. At the bottom left, there is a 'View Ownership Details' button.

Fig. 8 Copyright details page

Figure 8 displays the copyright details page of the platform. Along with browsing the copyrights on the home page, the users can also view the copyright details. When the user clicks the “view copyright details” button, the user is redirected to the copyright details page which displays all the information about the copyright such as owner name, copyright registration date, purchase cost, licensing cost, and created work. The users can also view the ownership histories of the copyright by clicking on the “view ownership details” button. Moreover, the users can easily redirect to the purchasing or licensing page by clicking on the “purchase” or “license” button available on the copyright details page.

5 Conclusions

The main objective of this paper is to design a blockchain-based copyright protection system through which users can register their created work on the platform and all the ownership transfer histories are constantly recorded on the tamper-proof distributed ledger with the help of smart contracts. This system ensures a high degree of decentralization eradicating the need for a central authority or third-party enterprises thus reducing the possibility of private tampering of data. The paper talks about the immutable and transparent nature of blockchain which makes the system tamper-proof and ensures trust among users through the transparency of blockchain technology. The system proposed in this paper not only lets users register their created work on to the platform, but also lets the users purchase the work or license the work for a specific duration for a set fee through the association of smart contracts. The transactions corresponding to both the parties are validated by nodes across the network and are stored on the blockchain network. Moreover, in this paper, an event response mechanism is designed to authenticate the identity of the parties involved

in a transaction. A log is maintained for storing all the events and the validity of the events is verified by the signatures carried in the event. Lastly, a decentralized application (Dapp) is built on top of the blockchain network based on the truffle framework. A local test network, Ganache is used to deploy and test the contract which runs in local memory therefore, swiftly approving transactions removing mining time and returning execution outcomes in actual time. To ensure user-friendliness of the Dapp, an interactive webpage interface is implemented for the proposed system, thus making it easier for the users to collaborate with the platform and blockchain network. According to the outcome of security analyses, data permanency, system independency, and protection from malicious attacks are ensured by our proposed system.

The proposed system model can be further enhanced in the future. Our future research work to optimize this copyright protection system includes (1) transfer of existing copyright records onto the blockchain network and (2) implementation of bots in blockchain-based copyright protection system using artificial intelligence to look for instances of the copyrighted work on the web making it easier for the copyright holder to find unauthorized users and file a case against them for compensation.

References

1. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Tech Rep [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
2. Bamert T, Decker C, Elsen L, Wattenhofer R, Welten S (2013) Have a snack, pay with bitcoins. In: Proceedings of 13th IEEE international conference on peer-to-peer computing (P2P'13), Sept 2013, pp 1–5
3. Lua EK, Crowcroft J (2005) A survey and comparison of peer-to-peer overlay network schemes. IEEE Commun Surv Tutor 7(2):72–93
4. Hofmann F, Wurster S, Ron E, Böhmecke-Schwafert M (2017) The immutability concept of blockchains and benefits of early standardization. In: 2017 ITU kaleidoscope: challenges for a data-driven society (ITU K), Nanjing, pp 1–8
5. Pilkington M (2015) Blockchain technology: principles and applications. In: Research handbook on digital transformations
6. Ethereum: a secure decentralised generalised transaction ledger—Dr. Gavin Wood Founder, Ethereum and Ethcore GAVIN@ETHCORE.IO
7. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: Proceedings of IEEE BigDataCongress'17, Honolulu, HI, USA, June 2017, pp 557–564
8. Buterin V (2013) Ethereum white paper: a next-generation smart contract and decentralized application platform
9. Technical Report, Survey on blockchain technologies and related services, Dec 2017 [Online]. Available: <http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf>
10. https://docs.corda.net/_static/corda-introductory-whitepaper.pdf
11. Gheith A, Rajamony R, Bohrer P, Agarwal K, Kistler M, Eagle BW, ... Kaplinger T (2016) IBM Bluemix mobile cloud services. IBM J Res Dev 60(2–3):7–1
12. Androulaki E, Barger A, Bortnikov V, Christian C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y, Muralidharan S, Murthy C, Nguyen B, Sethi M, Singh G, Smith

- K, Sorniotti A, Stathakopoulou C, Vukolić M, Cocco SW, Yellick J (2018) Hyperledger fabric: a distributed operating system for permissioned blockchains
13. Morgan JP (2016) Quorum whitepaper. <https://github.com/jpmorganchase/quorum-docs>
 14. Armknecht F, Karame GO, Mandal A, Youssef F, Zenner E (Aug 2015) Ripple: overview and outlook. In: International conference on trust and trustworthy computing. Springer, Cham, pp 163–180
 15. Schütte J, Fridgen G, Prinz W, Rose T, Urbach N, Hoeren T, Guggenberger N, Welzel C, Holly S, Schulte A, Sprengel P, Schwede C, Weimert B, Otto B, Dalheimer M, Wenzel M, Kreutzer M, Fritz M, Leiner U, Nouak A, Blockchain and smart contracts technologies, research issues and applications
 16. Waters R (June 2016) ‘Ether’ brought to earth by theft of \$50m in cryptocurrency. Financial Times, 18 June 2016
 17. Buterin V, A next-generation smart contract and decentralized application platform. <https://github.com/ethereum/wiki/wiki/White-Paper/>
 18. Wood G (2014) Ethereum: a secure decentralised generalised transaction ledger. gavwood.com/paper.pdf. Last accessed 10 Jan 2020
 19. Bartolini F, Piva A, Barni M (2002) Managing copyright in open networks. IEEE Internet Comput 6(3):18–26
 20. Manzalini A, Stavdas A (2008) A service and knowledge ecosystem for Telco3.0-Web3.0 applications. In: 2008 third international conference on internet and web applications and services, Athens, 2008, pp 325–329
 21. Atanasova I (2019) Copyright infringement in digital environment. J Law Econ 1:13–22
 22. Campidoglio M, Frattolillo F, Landolfi F (2009) The copyright protection problem: challenges and suggestions, pp 522–526
 23. Indrawan A, Stevens G, Brianto G, Gaol F, Oktavia T (2020) Legal protection of copyright on copyrighted content downloaded through the internet, pp 97–101. <https://doi.org/10.1145/3385209.3385228>
 24. Mane V, Khot N (2019) Copyright act, 1957: a study with reference to selected cases in India, pp 336–341
 25. Panda SK, Satapathy SC (2021) An investigation into smart contract deployment on Ethereum platform using Web3.js and solidity using blockchain. In: Bhateja V, Satapathy SC, Travieso-González CM, Aradhya VNM (eds) Data engineering and intelligent computing. Advances in intelligent systems and computing, vol 1. Springer, Singapore. https://doi.org/10.1007/978-981-16-0171-2_52
 26. Panda SK, Rao DC, Satapathy SC (2021) An investigation into the usability of blockchain technology in internet of things. In: Bhateja V, Satapathy SC, Travieso-González CM, Aradhya VNM (eds) Data engineering and intelligent computing. Advances in intelligent systems and computing, vol 1. Springer, Singapore. https://doi.org/10.1007/978-981-16-0171-2_53
 27. Jena AK, Dash SP (2021) Blockchain technology: introduction, applications, challenges. In: Panda SK, Jena AK, Swain SK, Satapathy SC (eds) Blockchain technology: applications and challenges. In: Intelligent systems reference library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_1
 28. Sathya AR, Panda SK, Hanumanthakari S (2021) Enabling smart education system using blockchain technology. In: Panda SK, Jena AK, Swain SK, Satapathy SC (eds) Blockchain technology: applications and challenges. In: Intelligent systems reference library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_10
 29. Mills DC, Wang K, Malone B, Ravi A, Marquardt J, Budev AI, Brezinski T et al (2016) Distributed ledger technology in payments, clearing, and settlement
 30. Lokre SS, Naman V, Priya S, Panda SK (2021) Gun tracking system using blockchain technology. In: Panda SK, Jena AK, Swain SK, Satapathy SC (eds) Blockchain technology: applications and challenges. In: Intelligent systems reference library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_16
 31. Panda SK, Mohammad GB, Nandan Mohanty S, Sahoo S (2021) Smart contract-based land registry system to reduce frauds and time delay. Secur Priv e172. <https://doi.org/10.1002/spy.2.172>

32. Panda SK, Satapathy SC (2021) Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers. *Pers Ubiquit Comput*. <https://doi.org/10.1007/s00779-021-01588-3>
33. Aldarwbi M, Al-Awami L (2019) A mechanism for copyright protection under information-centric networking, pp 1–6. <https://doi.org/10.1109/MENACOMM46666.2019.8988556>
34. Brassil J, Low S, Maxemchuk NF (1999) Copyright protection for the electronic distribution of text documents. *Proc IEEE* 87:1181–1196. <https://doi.org/10.1109/5.771071>
35. Ahmad T, Misra P (2011) E-commerce & its copyright issues. *SSRN Electron J*. <https://doi.org/10.2139/ssrn.1801782>
36. Liu X, Zha Y (2018) Copyright protection of digital movies using the coalition of technology and law in China. *Chin Stud* 07:259–276. <https://doi.org/10.4236/chnstd.2018.74023>
37. Jamali HR (2017) Copyright compliance and infringement in ResearchGate full-text journal articles. *Scientometrics* 112:241–254. <https://doi.org/10.1007/s11192-017-2291-4>
38. MengZ, MorizumiMiyataKinoshita (2018) Design scheme of copyright management system based on digital watermarking and blockchain. 2018IEEE 42nd annual computer software and applications conference (COMPSAC), Tokyo, 359–364
39. Solidity, Docs. <http://solidity.readthedocs.io/en/v0.4.24>
40. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S (Oct 2016) On the security and performance of proof of work blockchains. In: *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp 3–16
41. Kiayias A, Russell A, David B, Oliynykov R (Aug 2017) Ouroboros: a provably secure proof-of-stake blockchain protocol. In: *Annual international cryptology conference*. Springer, Cham, pp 357–388
42. Sankar LS, Sindhu M, Sethumadhavan M (Jan 2017) Survey of consensus protocols on blockchain applications. In: *2017 4th international conference on advanced computing and communication systems (ICRCCS)*. IEEE, pp 1–5
43. Fan X, Chai Q (Nov 2018) Roll-DPoS: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems. In: *Proceedings of the 15th EAI international conference on mobile and ubiquitous systems: computing, networking and services*, pp 482–484
44. Wang J et al (2019) A summary of research on blockchain in the field of intellectual property. *Proc Comput Sci* 147:191–197
45. Block. Global power distribution [EB/OL]. <http://www.qukuai.com/pools>, 25 June 2017
46. Jiang W, Jia (2017) Vernacular blockchain. Mechanical Industry Press, Beijing
47. Sabounchi M, Wei J (Nov 2017) Towards resilient networked microgrids: blockchain-enabled peer-to-peer electricity trading mechanism. In: *2017 IEEE conference on energy internet and energy system integration (EI2)*, pp 1–5. IEEE
48. Visual Studio Code. <https://code.visualstudio.com/>
49. Cui-Hong H (2012) Research on Web3.0 application in the resources integration portal. In: *2012 second international conference on business computing and global informatization*, Shanghai, pp 728–730

Secure Electronic Voting (E-voting) System Based on Blockchain on Various Platforms



K. Varaprasada Rao and Sandeep Kumar Panda

Abstract In today's world, online voting is becoming more popular. It has a lot of potential for lowering administrative expenses and increasing voter turnout. It eliminates the need for voters to travel to polling locations or print ballot papers because they can vote from anywhere with Internet criteria having been a struggle. In an E-voting system to provide security, we are using various cryptography techniques. In the existing E-voting system, all participants depend on a third-party entity for analysis and publishing of the voting results. To address this problem, many existing approaches use blockchain technology. These existing approaches face various problems like security issues and constraints on the number of voters. To address the two difficulties noted above, we offer a platform-agnostic, decentralized trust, and more secure E-voting mechanism that can be implemented on a platform-independent blockchain-based approach that supports smart contract execution.

Keywords E-voting · Blockchain · Security · Decentralization · Linkable ring signature · Paillier technology

1 Introduction

Election security is a concern of national security in any democracy. For more than a decade, the computer security industry has investigated the possibility of an E-voting system [1], to lower election costs while preserving and improving election security. Since the commencement of democratically electing candidates, the voting system has been based on pen and paper. A new election technology must replace the traditional pen and paper approach to eliminate fraud and make the voting process traceable and verifiable [2]. This is where blockchain technology comes into the

K. Varaprasada Rao (✉) · S. K. Panda
Department of Computer Science and Engineering, Faculty of Science and Technology, ICFAI
Foundation for Higher Education, Hyderabad, India
e-mail: varaprasad.fst@ifheindia.org

S. K. Panda
e-mail: sandeepanda@ifheindia.org

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023
S. C. Satapathy et al. (eds.), *Computer Communication, Networking and IoT*,
Lecture Notes in Networks and Systems 459,
https://doi.org/10.1007/978-981-19-1976-3_18

143

picture. Blockchain provides distributed decentralized data sharing among authorized users in a network [3]. Blockchain consists of collections of blocks, each block connected with the previous block and form like a chain [4].

These technological elements use modern encryption to provide a level of security equal to or greater than any other database. Several blockchain-based E-voting systems have recently been built by utilizing the technology's inherent capabilities.

2 Background and Literature Review

When Satoshi Nakamoto invented the first cryptocurrency, Bitcoin, in 2008, he introduced blockchain technology. The bitcoin blockchain technology combines a decentralized public ledger with a proof-of-work (PoW)-based stochastic consensus system, as well as financial incentives, to create a completely ordered sequence of blocks known as the blockchain. Nick Szabo coined the term "smart contracts" in the 1990s, describing them as "a set of promises, stated in digital form, including protocols within which the parties fulfill on these promises" [5]. A smart contract is a code that expresses logic, and it can operate as an unconditionally trusted third party [6]. It cannot be changed once it has been written, and all network members must check all stages. The beauty of smart contracts is that anyone with the ability to set up a blockchain node to confirm the results.

2.1 *Blockchain Architecture's Basic Elements*

The blockchain provides various basic components. Figure 1 describes the major components of blockchain are as follows.

Node: Node is a user or computer in the blockchain network.

Transaction: It's a unit of records in the blockchain network.

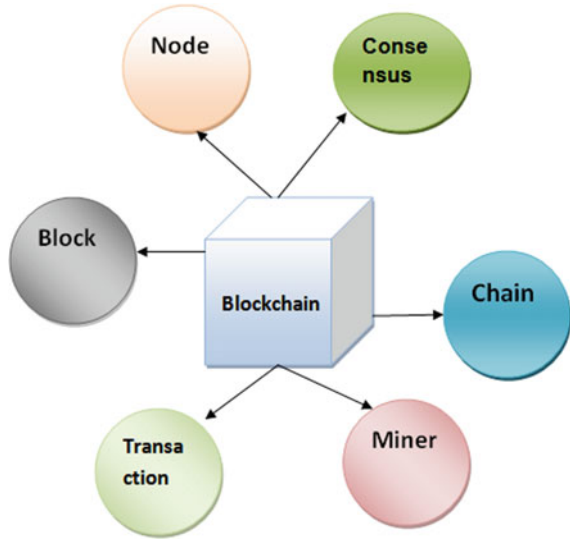
Block: It's a collection of data that are used to complete network transactions and distributed to all nodes.

Miners: in blockchain miners play a very important role to approve the transactions in the network [7].

Chain: A sequence of blocks in a specific order.

Consensus: A group of instructions that work together to complete blockchain procedures.

Fig. 1 Blockchain components



2.2 Blockchain Architecture's Crucial Characteristics

For all sectors that use blockchain, the architecture has numerous advantages. As shown in Fig. 2, there is a range of embedded characteristics:

Cryptography: It is used to provide security to each transaction in the blockchain network. **Immutability:** No changes or deletions can be made to blockchain records [2, 4, 8].

Decentralization: All participants of the blockchain network may have access to the complete distributed database. As seen in the core process, a consensus method enables system control [9–12].

Anonymity: Blockchain provides an address to every participant in the network [13].

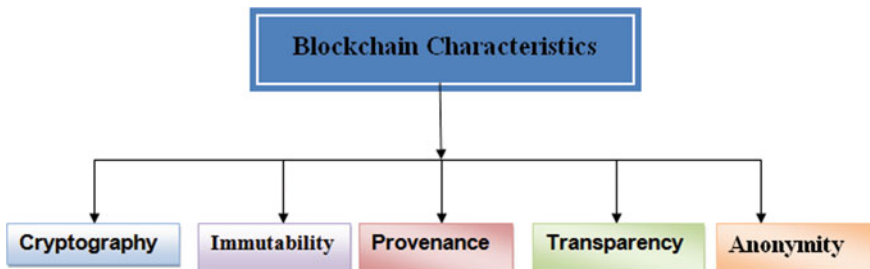


Fig. 2 Blockchain characteristics

Transparency: It means that the data in the network cannot be manipulated. It is not possible since erasing the blockchain network would need enormous computational resources.

2.3 *Review of Related Literature*

In recent years, several publications have been published that have highlighted various security and privacy issues in blockchain-based E-voting systems. Here, we present a few blockchain-based electronic voting techniques below:

Shahzad et al. [14] were proposed BSJC proof of completeness as a trustworthy electronic voting technique. They utilized a process model to describe the overall structure of the system. This approach addresses various security and privacy issues but this approach is capable of the small-scale election. However, a slew of other issues has been raised. The polling procedure may be delayed if the block is generated and sealed on a big scale [15–19].

Yi [20] presented the BES approach for proving security in an E-voting system in a P2P blockchain-based network. To prevent vote tampering, distributed ledger could be used. On UNIX systems in a peer-to-peer network, the system was tested and designed. Counter-measurement assaults are a key difficulty in this strategy. A distributed procedure, such as the use of secure multipart computers, may be able to solve the problem. However, if the computation function is sophisticated, and there are too many participants; computing costs become increasingly substantial and possibly prohibitive [21].

3 **Deployment of the System**

Our voting mechanism is compatible with any blockchain-based platform that supports smart contracts and achieves the same level of security [4, 15]. Other factors that may influence platform selection include vote latency and flexibility requirements [3]. In our scenario, we use the Hyperledger Fabric blockchain technology, which is based on Byzantine Fault Tolerance (BFT), to deploy our voting system in a real-world setting. Our approach supports the four requirements listed below.

1. **Encode and decode messages**

We need to encrypt the candidate ID before voting begins so that it is suitable for the vote count [22].

2. **Our voting mechanism does not depend on a centralized trustworthy entity to count polls and announce results**

The existing E-voting systems rely on a centralized third party to evaluate the polls and produce the results. In this approach, we use a blockchain decentralized approach to evaluate the ballots and produce the results [23].

3. **Our voting technology is platform agnostic and offers extensive security protections**

Our voting method is secure because it uses cryptographic approaches offered by our voting protocol; as a result, this approach is used in any smart contract-supported blockchain-based platform [24]. In this approach, Paillier technology is used to conduct the polling and provide privacy without revealing voter information, which helps us meet our goal of offering total security [25].

Generate Key: by using this function the voting administrator a secret key for every voter based on their public key [26].

Encryption: It is necessary to encrypt the plaintext ballot. This function is used to encrypt the voter polls during the blockchain network [27].

Decryption: By using this function, the voting administrator decrypts the votes polled by the voters and publishes the results.

Proof-of-work: This function is used to generate proof-of-work that indicates only authorized voter can encrypt their vote.

Decryption validates proof-of-work: By using this function, the voting administrator generates key-value pair to decrypt the votes and publish the polling results [20].

This function uses a linkable ring signature method to validate the voters and decrypt the votes, even if the owner of the ballot cannot be traced.

Linkable ring signature (LRS): LRS is used to preserve voters' privacy. By using this method, we use short linkable ring signature (SLRS), which eliminates constraints on the voting system. This LRS approach contains the following features: (1) check whether the voter is a valid user or not, (2) voters can verify whether their votes are polled by blockchain network or not, (3) to provide scalability maintain signature size, and (4) avoid double/duplicate voting. We use the tuple function in our voting system (Setup, KeyGen, Sign, Verify, Link).

4. **Our voting platform is adaptable and expandable:** We offer two optimized SLRS key accumulation methods that allow voting scalability and achieve latency in large-scale voting.

4 Voting Protocol

Figure 3 describes the architecture of the E-voting system; the voting system comprises various voters, vote administrator (VA), front-end smart contract server (SCA), and numerous smart contract validation nodes. A smart contract validation node's job is to accurately simulate the execution of smart contract codes. The validation nodes for practical voting could be controlled by many stockholders, implying that all ballots on the blockchain have been confirmed by various stockholders.

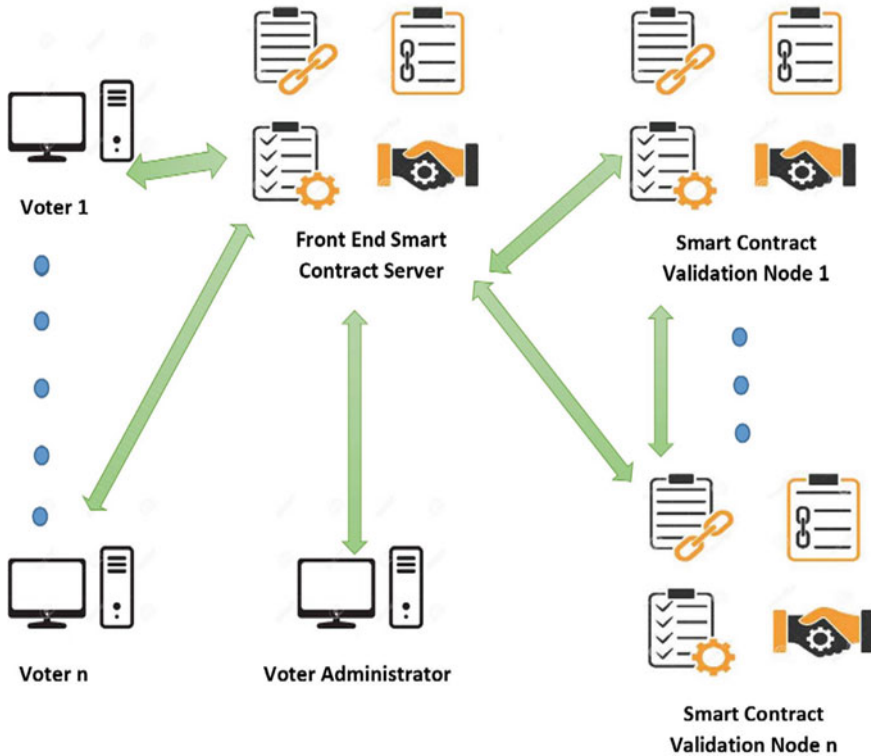


Fig. 3 Blockchain-based independent E-voting system

4.1 Voting Process Entities

In our voting system (shown in Fig. 3), there should be four entities participating, with the following details:

Smart Contract Administrator (SCA): SCA can access the blockchain platform and apply or terminate smart contracts. The membership service in Hyperledger Fabric authorizes this account, and the authority to apply or dismiss the smart contract is provided. In this approach, we required at least one SCA to install the voting smart contract.

Voter Administrator (VA): The VA manages the votes by establishing polling settings, initiating the counting and results in publication phases. SLRS is used to prevent administrators from associating ballots to users, although Hyperledger has underlying means for authenticating users.

Smart contract: A smart contract's job is to (1) store encrypted ballots. (2) Check the ballots for legitimacy. (3) Count the ballots that have been encrypted. (4) Verify that the vote results are valid. (5) Make the vote results public and gives a platform for people to check the results of the election.

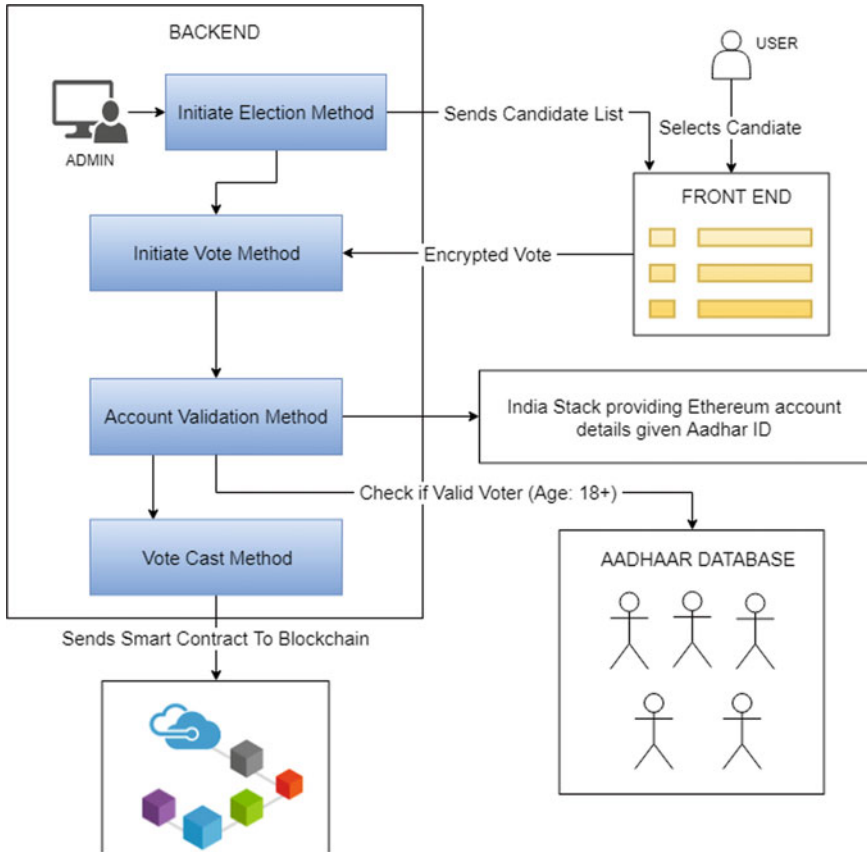


Fig. 4 Blockchain-based E-voting process

Voter: Voters are those who can exercise their right to vote. Before anyone can vote, individuals must first register with the voting system.

Figure 4 describe the E-voting system process using blockchain.

4.2 Registration of Voters

The user must register his identification using this voting mechanism. The registration information could include: (1) Email Id and password, (2) voter Id and password, (3) an administrator-sent invitation URL with the desired password. After passing the savvy agreement’s personality check, the client can sign in with the ideal secret key to download the SLRS param and the executive public key, then, calls the KeyGen() function to produce the SLRS key pair (); then the user transfers the public key to

the ballot. If his SLRS public key is acknowledged, the shrewd agreement puts his public key on the blockchain, finishing his/her enrollment step.

5 Conclusions

E-voting is a method of casting and tallying votes that use computers. It is a time- and cost-effective method of conducting a voting operation, with the advantages of large amounts of data in real time and a high level of security. It takes out the requirement for citizens to go to surveying areas or print voting form papers since they can cast a ballot from any place with Internet standards that have been a battle. In the existing E-voting system, all participants depend on a third-party entity for analysis and publishing of the voting results. To resolve the issue that the current blockchain casting a ballot framework needs thorough security highlights, and most of them are stage subordinate, we proposed a blockchain-based democratic framework in which electors' protection and casting a ballot accuracy are ensured by homomorphic encryption, linkable ring marks, and proof-of-work between the citizen and blockchain. Our approach eliminates security attacks and eliminates the constraints on the number of voters and candidates supported during polling and provides secure architecture. Our voting system's correctness and security are examined. This approach provides that our voting method performs well even in large-scale voting.

References

1. Alaya B, Laouamer L, Msilini N (2020) Homomorphic encryption systems statement: trends and challenges. *Comput Sci Rev* 36:100235
2. Murala DK, Panda SK, Swain SK (2019) A novel hybrid approach for providing data security and privacy from malicious attacks in the cloud environment. *J Adv Res Dyn Control Syst* 11(06-Special Issue)
3. Liu Y, Wang Q (2017) An E-voting protocol based on blockchain. *IACR CryptolEprint Arch* 1043, Racsco P (2019) Blockchain, and democracy. *Soc Econ* 41:353–369
4. Murala DK, Panda SK, Swain SK (2019) A survey on cloud computing security and privacy issues and challenges. *J Adv Res Dyn Control Syst* 11(06-Special Issue)
5. Szabo N (2017) Formalizing and securing relationships on public networks. *First Monday* 1997, 2, 9. *The Economist*. EIU Democracy Index. 2017. Available online: <https://infographics.economist.com/2018/DemocracyIndex/>. Accessed on 18 Jan 2020
6. Fernández-Caramés TM, Fraga-Lamas P (2020) Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access* 8:21091–21116
7. Zhao Z, Chan T-HH (2016) How to vote privately using Bitcoin. In: Qing S, Okamoto E, Kim K, Liu D (eds) *ICICS 2015*, vol 9543. LNCS. Springer, Cham, pp 82–96
8. Murala DK, Panda SK, Swain SK (2019) Secure dynamic groups data sharing with modified revocable attribute-based encryption in cloud. *Int J Recent Technol Eng (IJRTE)* 8(4), Nov 2019. ISSN: 2277-3878
9. Yu B et al (2018) Platform-independent secure blockchain-based voting system. *Cryptology ePrint Archive*, change me (2018). <http://eprint.iacr.org/201>

10. Panda SK, Satapathy SC (2021) An investigation into smart contract deployment on Ethereum platform using Web3.js and solidity using blockchain. In: Bhateja V, Satapathy SC, Travieso-González CM, Aradhya VNM (eds) Data engineering and intelligent computing. Advances in intelligent systems and computing, vol 1. Springer, Singapore. https://doi.org/10.1007/978-981-16-0171-2_52
11. Panda SK, Rao DC, Satapathy SC (2021) An investigation into the usability of blockchain technology in internet of things. In: Bhateja V, Satapathy SC, Travieso-González CM, Aradhya VNM (eds) Data engineering and intelligent computing. Advances in intelligent systems and computing, vol 1. Springer, Singapore. https://doi.org/10.1007/978-981-16-0171-2_53
12. Sathya AR, Panda SK, Hanumanthakari S (2021) Enabling smart education system using blockchain technology. In: Panda SK, Jena AK, Swain SK, Satapathy SC (eds) Blockchain technology: applications and challenges. Intelligent systems reference library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_10
13. Gao S, Zheng D, Guo R, Jing C, Hu C (2019) An anti-quantum E-voting protocol in blockchain with audit function. *IEEE Access* 7:115304–115316
14. Shahzad B, Crowcroft J (2019) Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access* 7:24477–24488
15. Lai WJ, Hsieh YC, Hsueh CW, Wu JL (2018) Date: a decentralized, anonymous, and transparent e-voting system. In: Proceedings of the 2018 1st IEEE international conference on hot information-centric networking (HotICN), Shenzhen, China, 15–17 Aug 2018
16. Jena AK, Dash SP (2021) Blockchain technology: introduction, applications, challenges. In: Panda SK, Jena AK, Swain SK, Satapathy SC (eds) Blockchain technology: applications and challenges. Intelligent systems reference library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_1
17. Lokre SS, Naman V, Priya S, Panda SK (2021) Gun tracking system using blockchain technology. In: Panda SK, Jena AK, Swain SK, Satapathy SC (eds) Blockchain technology: applications and challenges. Intelligent systems reference library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_16
18. Panda SK, Mohammad GB, Nandan Mohanty S, Sahoo S (2021) Smart contract-based land registry system to reduce frauds and time delay. *Secur Priv* e172. <https://doi.org/10.1002/spy.2.172>
19. Panda SK, Satapathy SC (2021) Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers. *Pers Ubiquit Comput*. <https://doi.org/10.1007/s00779-021-01588-3>
20. Yi H (2019) Securing e-voting based on blockchain in the P2P network. *EURASIP J Wirel Commun Netw*
21. Hopwood D, Bowe S, Hornby T, Wilcox N (2016) Zcash protocol specification. Technical report, 2016–1.10. Zerocoin Electric Coin C
22. Tivi Voting. <https://tivi.io/>. Accessed 24 June 2017
23. Torra V (2019) Random dictatorship for privacy-preserving social choice. *Int J Inf Secure* 19:537–543
24. Tsang PP, Au MH, Liu JK, Susilo W, Wong DS (2010) A suite of non-pairing IDbased threshold ring signature schemes with different levels of anonymity (extended abstract). In: Heng S-H, Kurosawa K (eds) *ProvSec 2010*, vol 6402. LNCS. Springer, Heidelberg, pp 166–183
25. Jafar U, Ab Aziz MJ, Shukur Z, Blockchain for electronic voting system—review and open research challenges
26. Wood G (2014) Ethereum: a secure decentralized generalized transaction ledger. *Ethereum Proj Yellow Pap* 151:1–32
27. Yaga D, Mell P, Roby N, Scarfone K (2020) Blockchain technology overview. *arXiv* 2019. [arXiv:1906.11078](https://arxiv.org/abs/1906.11078). The Economist. EIU Democracy Index, 2017. Available online: <https://infographics.economist.com/2018/DemocracyIndex/>. Accessed on 18 Jan 2020

Dynamic Authentication Using Visual Cryptography



K. D. Devika and Ashutosh Saxena

Abstract Nowadays with the increase in cybersecurity threats, it has become very important to upgrade the cybersecurity standards for all web applications. Especially in the area of Internet Banking, user authentication is a major issue. An extra layer of security is necessary for user authentication. Two-factor authentication is providing extra layer security in banking services. Biometric-based authentication, password-based authentication, smart card-based authentication are some of the authentication techniques used in banking systems. But all these techniques rely on the security of the database. Another issue faced by the users is regarding the latency in receiving the SMS OTP during online banking. If the network connection is poor, then the user may face latency in receiving OTP. To overcome these issues, we can use the concept of visual cryptography. This paper aims to use the “visual cryptography technique” for the authentication of a user in Internet Banking systems. Visual cryptography was proposed by Naor and Shamir (Naor M, Shamir A (1995) Visual cryptography. In: Proceedings of the advances in cryptology—Eurocrypt) in 1994. VC is one of the most secure techniques which can be used for secret sharing, in which the secret information will be in the form of an image. During encryption, we can divide the image into different shares or transparencies and the decryption process can be done by superimposing the shares. There is no need for complex computations in decryption; even by using a normal human visual system, we can decrypt the image; this is one of the advantages of visual cryptography. This paper presents a technique that uses the concept of (2,2) VC scheme to create shares of a unique key generated during the time of customer account creation. One of these shares is given to the

Part of this work was submitted as Masters Project to University of Hyderabad, Hyderabad.

K. D. Devika (✉) · A. Saxena
CRRAO-AIMSCS, University of Hyderabad Campus, Hyderabad, India
e-mail: devikakd405@gmail.com

A. Saxena
e-mail: saxenaaj@gmail.com

A. Saxena
CMR Technical Campus, Hyderabad, India

customer, and another share will be kept within the server. During the time of two-factor authentication instead of OTP, OTP positions will be generated, and according to that, the server-side share will undergo changes dynamically. And the server-side share will be displayed to the user. The user can superimpose his/her share with the server share to generate the OTP.

Keywords Visual cryptography · One-time password · SMS—short message service

1 Introduction

Internet Banking plays a major role in our day-to-day life. User authentication is one of the most important challenges faced in Internet Banking. In order to provide access to the users personal data, Internet Banking allows remote login for users. Two-factor authentication can provide extra layer of security in the user authentication process. One-time passwords (OTP) are used in two-factor authentication. OTP is used to validate the user for a particular login session. Normally, OTPs are transmitted through SMS. Wireless interception, smartphone Trojans, SIM swap attacks, etc. are some of the attacks possible on SMS-OTP transmissions. Due to the congestion in the network, latency in SMS-OTP is another major issue. If the SMS gateway is facing some issues or if it is under maintenance, users may face latency in receiving the SMS-OTP. For roaming users (traveling abroad) depending on the operator, there can be restrictions in accessing services. The services of SMS-based authentication methods may be blocked in some sensitive and emergency situations where the government may dictate a blockage of this service. When a mobile phone [1] creates a data connection, in some situations, it cannot receive SMS messages, and users might not be conscious of this.

SIM card hacking is becoming one of the serious security threats mainly in two-factor authentication systems. Through SIM card hijack, the attackers get the user's account, financial, and personally identifiable information (PII). On-line accounts and transactions can be compromised easily with a hacked SIM card. SIM swap and SIM clone are the two main techniques used in SIM hijacking. These attacks are targeting normal middle-class people to high-profile people. In 2019, Twitter CEO "Jack Dorsey" faced a SIM swapping incident.

To overcome the problems associated with SMS-based OTP transmission, this paper proposes a technique using (2,2) VC scheme [2–9]. It is a basic VC scheme in which a secret image is divided into two shares or two transparencies. And the secret can be recovered by superimposing both the shares together. Individual transparencies cannot give any idea regarding the secret present in it.

Here, a key (a randomly generated $10 * 10$ matrix) in the form of an image will be divided into two shares using (2,2) VC scheme. One share will be kept on the server-side and another share will be given to the user. During authentication, a one-time password will be generated and according to that server-share will change and

display to the user. Users can superimpose his/her share with the share displayed or provided by the server. And the user can read the OTP and finish the transaction.

2 Current Trends in One-Time Passwords

In the early 1980s, the American scientist Leslie Lamport proposed the idea of a one-time password [10–12]. An OTP is a dynamically created numeric or alphanumeric sequence of characters which will be valid for only one authentication session. OTPs are much more secure than user created static passwords that can be weak or used in multiple platforms. OTP systems greatly reduce the chances of phishing attacks, replay attacks, etc. which are possible to occur on normal password-based authentication. There are several methods for generating and transferring OTP to the users. Short message service (SMS), proprietary tokens, grid cards and software tokens are some of the techniques.

2.1 SMS-Based OTP

The SMS-based OTP [12, 13] transmission mechanism is widely utilized. SMS is often regarded as one of the most effective data transport techniques. Other than mobile phones, no other device is required, no additional hardware is required, and the cost is minimal, to name a few advantages of utilizing SMS for OTP transmission. However, it is riddled with flaws. Wireless eavesdropping, mobile phone Trojans, SIM SWAP assaults, and other threats are all possible.

Wireless interception: Wireless attacks [12, 13] are done by keeping an unauthorized device on the wireless network that carry out a security process. Femto cells are used in most cases for this purpose. Voice calls, inbound SMS, and MMS messages may all be recorded with these femto cells. Because of poor encryption methods and a limitation of mutual authentication, GSM technology [13] used to transmit SMS to the intended user is deemed unsafe.

Mobile phone malware: SMS OTP Trojans [12–17] are malicious programs that the user installs. The ZITMO (Zeus In The MOBILE) Trojan for Symbian OS is the world's first virus designed exclusively to intercept Mobile Transaction Authorization Number (mTANs). It is made to steal the one-time passwords (OTPs) that banks provide in text messages. Its primary goal is to send incoming text messages with mTAN codes to malicious recipients. A Zeus variant for mobile phones with windows OS was discovered in February 2011 and dubbed Trojan-Spy WinCE.Zbot.a. The collaboration between ZITMO and the original PC-based Zeus Trojan is its most distinguishing characteristic.

SIM swap attack: SIM swapping [13, 15, 16] is the next stage of phishing scam. After acquiring the basic private information of the user through phishing, the attacker can intercept calls and SMS coming to the user's mobile. It is a kind of spear phishing

attack. The attacker uses social engineering technique to misguide the user's mobile operator to port the user's mobile number to the SIM which the attacker has. The attacker then starts receiving messages and incoming calls including the OTPs sent by the bank. The attacker can perform transactions in the user's bank account by using the personal information collected through phishing and key logging and also with the SMS-OTP.

SIM clone attack: SIM cloning [14–17] is a method similar to SIM swapping used by attackers to make a duplicate of the target's SIM. Cloning is the process of creating a duplicate of the real SIM card by using smart card copying.

Cloning is the process of creating a duplicate of real SIM card by using smart card copying software. As a result of this, the attacker will be able to obtain the victim's international mobile subscriber identification (IMSI) and master encryption key.

This approach involves inserting the original SIM card into a card reader and copying the data from there. SIM cards may also be remotely hacked via over-the-air (OTA) connectivity to compromise updates sent to SIM through SMS. The attacker then calls the victim and requests to restart his phone with in a certain amount of time. When the victim's phone is turned off, the assailant turns on his phone. When the victim restarts his phone, the activity will be over. SIM jacker is a surveillance tool used by the attacker in past to clone SIM cards. SIM application toolkit (STK) and SIM alliance toolkit (S@T) browser technologies are installed on SIM cards, and the tool utilizes instructions to access them. It allows attackers to obtain sensitive information about the device, such as its position.

SMS transmission latency: Another major issue with SMS-OTP is associated with the transmission latency [14, 17]. Due to congestion in the network, an increase in latency for SMS transmission is a common problem. Issues with mobile devices such as inbox are full, or the mobile application is frozen can also be a cause of increased latency. If sender and receiver use different networks, there is a probability that the messages will be delayed since each network prioritizes its own traffic. Also for a roaming number, delivery is not guaranteed.

2.2 Proprietary Tokens

With proprietary tokens [17], users need to carry a device that is responsible for creating and displaying OTP. A proprietary token is a security token that looks like a small calculator or a key chain charm with an LCD that shows a number that changes occasionally. There is an accurate clock inside the token that has been synchronized with the clock on the proprietary authentication server.

The issue associated with this hardware token is availability and replacement. These devices are not user serviceable and require replacement once in at least three year.

2.3 Grid Cards

Grid cards [17] are two-factor authentication tokens. It is simple, secure and cost effective. Grid cards are based on security grids. Security grid has a matrix with random letters and numbers in rows and columns. In small credit card sized plastic cards, these grids are printed. Carrying grid cards safely is an issue associated with this technique.

2.4 Software Tokens

Software tokens [17] are software programs capable of generating one-time passwords. They have a lot of advantages than hardware tokens. We can use soft tokens through some smart phone applications, so that we can use it anywhere in the world; also it is easy to update, the cost of additional token is negligible, and it can be distributed to users instantly. Google authenticator, Authy, etc. are some of the software token examples.

3 Proposed Methodology

In the proposed system, a key in the form of a $10 * 10$ matrix is generated randomly. For each user, a unique key matrix is generated in the form of an image (Fig. 1) at the time of account creation. Each row and column of the matrix contains numbers from 0 to 9 without repetition. Two shares (Fig. 2) (a user share and a server share) of the generated key will be created using (2,2) visual cryptography [18–22]. The user share will be given to the user and the server share will be kept in the bank server side. The user share will be a static share that is not needed to change in any point of time.

A sequence of numbers of any length between 1 and 100 will be generated randomly during user authentication. These numbers represent the positions of digits in the key. These corresponding digits will form the random OTP (Fig. 3). Changes in server-side share are made according to the generated sequence of numbers; i.e., an extra layer of gray-scale cover (Fig. 4) will be used to hide the positions other than the generated sequence.

This created server-side share will be displayed or given to the user. And the user can superimpose this given share with the share which the user already has. Then the user will be able to see the OTP (Fig.5). By using that, user can do further transactions.

3.1 Proposed System Merits

- An OTP of length between 1 to 100 numbers of digits can be generated.
With the increase in number of OTP digits, security can be increased.
- Individual shares or transparencies cannot give any idea about the hidden secret.
- Latency will be very less compared to normal SMS-OTP methods.
- More protected than SMS-OTP method because of the use of encrypted shares.
- By using any easy image superimposition technique (e.g.: Power point), the secret can be decrypted.
- User-friendly. There is no need for any prior knowledge of technologies.

3.2 Proposed System Demerits

- Both shares should be kept properly (alignment should be proper) one upon the other for decryption.
- The server share transparency should be 50 to get the secret visible.
- Proper Internet connection is required.

4 Experiment Results

Generated user key (Fig. 1).

User share and server share generated after encryption (Fig. 2).

Randomly generated OTP positions (Fig. 3).

Fig. 1 User key

6	4	0	5	2	8	1	3	9	7
9	2	1	0	8	4	3	7	5	6
3	1	8	0	6	4	9	5	7	2
9	0	1	4	8	7	3	2	6	5
6	0	9	7	5	8	2	3	1	4
3	4	7	8	0	2	9	1	5	6
8	4	7	2	6	3	0	1	5	9
8	9	1	7	5	0	3	6	4	2
7	5	9	4	3	2	1	6	0	8
9	0	3	4	8	1	2	5	7	6

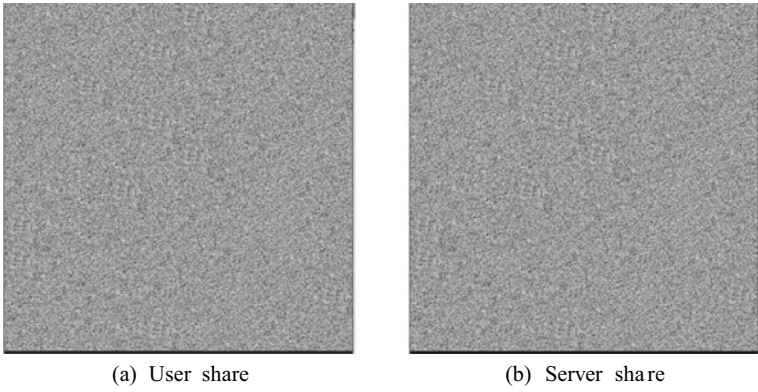
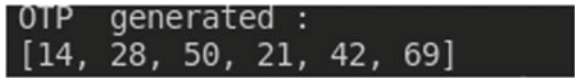


Fig. 2 Generated user and server shares

Fig. 3 OTP positions



Dynamic server share (Fig. 4).

Decrypted image (Fig. 5).

Fig. 4 Dynamic server share

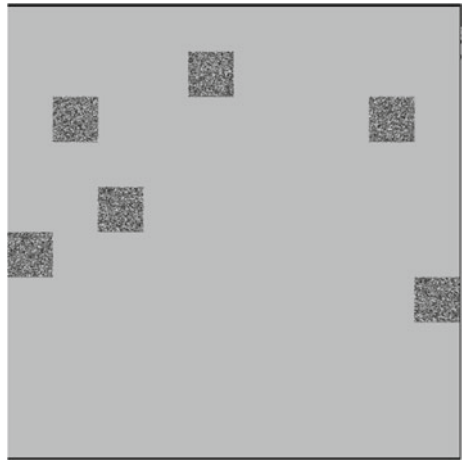
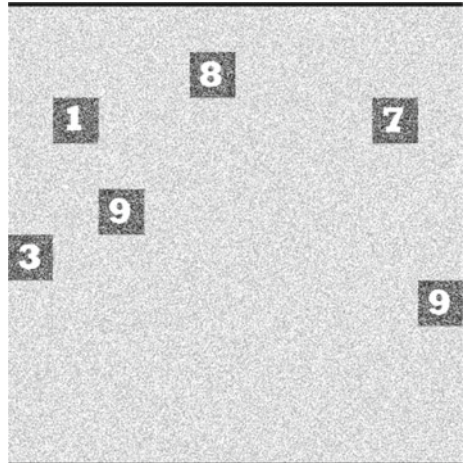


Fig. 5 Combined image

5 Conclusion and Future Works

5.1 Conclusion

In this paper, we are trying to introduce a secure method for user authentication in Internet Banking using the concept of visual cryptography. Here, a key in the form of a $10 * 10$ matrix is generated and divided into two shares using $(2,2)$ VC scheme. The user share will be a static share and the changes are made in the server-side share according to the OTP generated. Decryption can be done easily by superimposing both shares. This method has many advantages over the conventional SMS-OTP method. It is less vulnerable to attacks compared to SMS-OTP method, and it can greatly reduce the latency problems associated with SMS-OTP.

5.2 Future Work

A simple mobile application can be developed to overlay the two shares. This will help the user to quickly scan and superimpose the server's share with their own share. This application needs three essential features: a camera, an image file(jpg, png, jpeg) reader, and an image overlapping feature. Also we can make use of this similar mechanism in all other applications which require two-factor authentication.

References

1. Saxena A, Das ML, Gupta A (2005) MMPS: A versatile mobile-to-mobile payment system. In: 2005 4th annual international conference on mobile business, ICMB 2005, pp 400–405 (12)
2. Naor M, Shamir A (1995) Visual cryptography. In: Proceedings of the advances in cryptology—Eurocrypt, pp 1–12. <https://doi.org/10.1007/BFb0053419>
3. Nakajima M, Yamaguchi Y, Extended visual cryptography for natural images. *J WSCG* v10(i2):303–310
4. Hou YC, Chang CY, Lin F (1999) Visual cryptography for color images based on color decomposition. In: Proceedings of the fifth conference on information management, Taipei, Nov 1999, pp 584–591
5. Zhou Z, Arce GR, Dicrescenzo G (2006) Halftone visual cryptography. *IEEE Trans Image Process* 15(8):2441–2453
6. Kang I, Arce GR, Lee HK (2009) Color extended visual cryptography using error diffusion
7. Dhole AB, Janwe NJ (2013) An implementation of algorithms in visual cryptography in images. *Int J Sci Res Publ* 3(3), March 2013, ISSN 2250-3153
8. Chandramati S, Ramesh Kumar R, Suresh R, Harish S (2010) An overview of visual cryptography
9. Parakh A, Kak S, Recursive threshold visual cryptography scheme. <https://www.researchgate.net/publication/24009070>
10. Haller Bellcore N, Metz C (1996) A one-time password system. Kaman Sciences Corporation, May 1996
11. Zhou Y, Hu L, Chu J (2017) An enhanced SMS-based OTP scheme. advances in engineering research. In: 2nd international conference on automation, mechanical control and computational engineering (AMCCE 2017), vol 118
12. Mulliner C, Borgaonkar R, Stewin P, Seifert J-P, SMS-based one-time passwords: attacks and defense
13. Ammayappan K, Saxena A, Negi A (2006) Mutual authentication and key agreement based on elliptic curve cryptography for GSM. In: 2006 proceedings—2006 14th international conference on advanced computing and communications, ADCOM 2006, pp 183–186
14. Hamdare S, Nagpurkar V, Mittal J (2014) Securing SMS based one time password technique from man in the middle attack. *Int J Eng Trends Technol (IJETT)* 11(3), May 2014.
15. Agoyi M, Seral D, SMS security: an asymmetric encryption approach. In: 2010 sixth international conference on wireless and mobile communications
16. Ankita, Karia R, Patankar AB, Tawde P (2014) SMS-based one time password vulnerabilities and safeguarding OTP over network. *Int J Eng Res Technol (IJERT)* 3(5), May 2014. ISSN: 2278-0181
17. <https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/smsotp.html>
18. Prachi, Rathod D, Kapse SR, Secure bank transaction using data hiding mechanisms
19. Jain A, Soni S, Visual cryptography and image processing based approach for secure transactions in banking sector
20. Pal JK, Mandal JK, Dasgupta K, A (2, N) visual cryptographic techniques for banking applications
21. Hegde C, Manu S, Deepa Shenoy P, Venugopal KR, Patnaik LM, Secure authentication using image processing and visual cryptography for banking applications
22. <https://github.com/Ferruck/viscrypt.git>

Browser Extension for Digital Signature



Yerra Maithri and Ashutosh Saxena

Abstract In the current era, it is most crucial for the organisations to expand their operations in the market environment and economic situations for consumers and partners. Here, digital security plays an important role in establishing the trust between the enterprises and the consumers [1]. To secure the web content, at present, we are using secure socket layer (SSL) over HTTP. However, SSL tackles only a subset of security services. SSL does not offer non-repudiation services which is also an equally important security requirement. This non-repudiation service can be achieved by digital signatures. This digital signature technology helps us not only to have non-repudiation services but also to have integrity and authentication services. The problem here is integration of digital signatures into web applications which is not easy as there are multiple signature (Shailaja G, Phani Kumar K, Saxena A in Universal designated multi verifier signature without random oracles, pp. 168–171, 2006) [2] representations and different key storage formats. But we need to have a standardised approach to consume the underlying PKI services. Except the vendors adhere to the formats which are standard meticulously, interoperability between applications cannot be always guaranteed. To achieve these standard formats, we use various available PKCS standards developed by RSA Laboratories. The key requirements here are signature creation and verification, centralised architecture and flexibility to sign the web content. PKCS7 standard which is named as “Cryptographic Message Syntax Standard” is extensively used for the verification of digital signatures and certificates. For example, S/MIME uses this standard as the basis. PKCS12 [3] standard which is named as “Personal Information Exchange Syntax Standard” describes about transfer syntax for personal identity information, private keys and certificates. In this paper, the main aim is to discuss how to get signed the

Part of this work was submitted as Masters project to University of Hyderabad, Hyderabad.

Y. Maithri · A. Saxena (✉)
CRRAO-AIMSCS, University of Hyderabad Campus, Hyderabad, India

Y. Maithri
e-mail: maithriyerra@gmail.com

A. Saxena
CMR Technical Campus, Hyderabad, India

web content in its entirety or selectively with the help of a browser extension such that it provides digital signatures and integrity services to the web content and also provides convenience to the end-users to use these security services.

Keywords Digital signature · Digital certificate · Browser extension

1 Introduction

In the currently growing business environment, it is more important to secure web content as people are extensively using the Internet for every need and sharing sensitive information across the web. Enterprises must extend their services to consumers, employees and partners. Hence, it is important for the enterprises and consumers to build trust and credibility among each other. Trust is the most crucial underlying principle of security. Digital signatures play an important role in building this trust and credibility. Digital signature technology helps us to address non-repudiation, in addition to integrity and authentication services. It is important to take into consideration the privacy and integrity of the data which is in transit. In the current scenario, to secure the web content, we are using HTTPS, i.e. HTTP over SSL. It encrypts as well as decrypts the page requests of the user and also those pages which server returns to the user, and it also supports the authentication of the sender. A private connection that is reliable can also be established by HTTP over SSL. But only these things cannot offer complete security. An equally important security service which must be provided without compromising is non-repudiation. Digital signatures provide non-repudiation service as well as authentication and integrity services.

1.1 Importance of Digital Signature

Digital signature plays a very important role in the world today as almost all the services has become online. To render the services to the customers in a secured manner, security measures has to be taken. To provide these security services, we use digital signature in many applications.

In many countries, e-governance is the latest trend and the rise of this system is the most striking development of the web. In this system, government is online to provide its services to the citizens [4]. These services can be from government to citizen, government to business, government to employee or vice versa. People can access these services from anywhere and anytime. However, as these services are online, providing security is the biggest concern. Government also implements many projects in which data has to be protected from the intruders or unauthorised users. Hence, for successful implementation of such projects, security plays an important role. We can use digital signature technique [5] to authenticate and verify the electronic transactions.

Not only in e-governance but also in e-commerce digital signature plays an important role. The transformation of the current world forces businesses to handle their services in a quick, convenient, efficient and in a highly secured manner so that they can trade goods. Both the customers and service providers must ensure that the online transactions are real and reliable operations and also should have absolute confidence in the whole process. So to handle these services, digital signature can be used.

In the past, businesses had adopted hand signature and company's seal for signing contracts, taxes, transactions, etc. In the banking sector also, every transaction requires a personal signature. These processes require a lot of time for its implementation and also requires to maintain a lot records. To improve this situation, digital signatures can be used which handles security and improves efficiency.

1.2 Importance of Certificate-Based Digital Signature

The development technology in general has increased the demand of individuals for various services. The same is applied for digital signatures. Currently, digital signature is being used in many applications but the main problem encountered when it is applied for the web applications. The main issue raised when the digital signature is being tried to be developed to sign the web content and also the compatibility of the browsers is also considered. In a public key cryptosystem, every user has a public key and also a private key, where the public key is announced to everyone and a private key must be kept secret. However, here the problem is public keys can be tampered by any malicious third party. So, to overcome this, we use digital certificates which contain the key pair along with the user identity. The theory and technology base of certificate-based digital signature is public key infrastructure (PKI) [6]. PKI is an arrangement which consists of certificate authority (CA), certification library, secret key backup system as well as restore system, certification withdrawal method, etc. as well as provides services which can encrypt public key and also digital signatures on the basis of public key encryption mechanics. CA be the main part as far as PKI is concerned. It provides services such as withdrawing, updating and validating certificates. PKI is mainly formulated on cryptographic theory and delivers services such as confidentiality, integration, authenticity as well as non-repudiation services [7]. The role of digital certificate is similar to the role of identification card in real life. It contains the name of the identity, public and private key pair and some metadata relating to the digital certificate.

The concept of certificate is central to modern software security. Web browsers generally secure the traffic by using digital cryptography algorithms. Broadly speaking, there are two types of algorithms, i.e. same key cryptography and asymmetric key cryptography. In same key cryptography, as the name says, same key is applied for both encryption as well as decryption. In public key cryptography, a public and private key pairs are generated, and the public key is distributed. Public key is used for encryption, and private key is used for decryption. This allows parties to exchange information over an unsecured channel. However, there is a problem of public keys

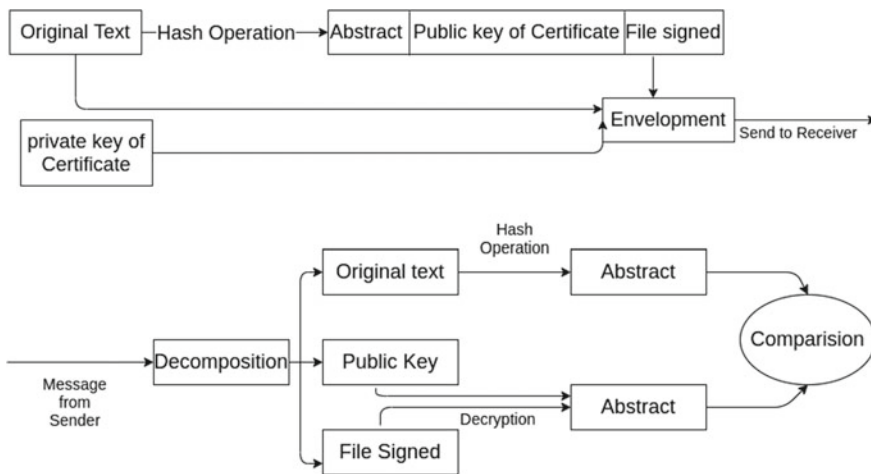


Fig. 1 Process of signature and verification with certificate

getting tampered by a malicious third party. Here comes the concept of public-key-infrastructure (PKI). PKI be a set, which is composed of trusted endorsement which can affirm the validity of a public key [7]. If the public key is tampered, the trusted authority can detect this and warn [7]. The structure of the digital certificate-based digital signature is as follows (Fig. 1).

2 Digital Signature Based on Digital Certificate

Digital signature is a mathematical technique used for authentication, integrity and non-repudiation service. It is digitally equivalent to a handwritten signature but it offers far more inherent security. They can provide evidence of origin, identity and status of digital messages.

Here, we use digital certificate-based signatures. Unlike conventional handwritten signatures, a signature which is set-up on the basis of certificate is laborious to replicate because it holds within the information which is encrypted that is specific to the signatory [8]. We use certificate-based signatures to send data to an external recipient for signature using digital certificates to increase legal compliance.

The number of individuals and the businesses that make use of the Internet to transmit data is increasing as it is faster, convenient and affordable. The problem is that the Internet is not designed by keeping security in mind. To facilitate secure electronic transfer of information, a set of policies and procedures was implemented to manage public key encryption. The main problem in a public key system is to prove that the public is genuine and authentic and has not been tampered by any third party. Here, digital certificates play an important role. They are supplied alongside a trusted certificate authority (CA) which binds together the same key and the identity of the

user. This kind of system is mentioned as public key infrastructure (PKI). Without digital certificates it would not be possible for two parties to share their public key in an authenticated way [8]. Benefits of digital certificates are authentication, integrity, confidentiality, easy to manage and easy to implement.

The challenges in implementing digital signatures on the web is that the digital signature uses the digital certificate of the current user, which is stored on a local storage or file which has restricted access [9]. Here, we use a pfx file to store the digital certificate. PKCS12 be a binary format which is used to cache the certificate of the server [10], any certificates which are intermediate and secret key into a single file that is encryptable.

2.1 *Creating a pfx Certificate*

Generation of RSA secret key by using the command which is as follows: `openssl genrsa -out private-key.pem 3072`

It is using a 3072-bit length key. This gives a file called as PEM which consists of an RSA secret key. Now, we have a private key, by using this, we can generate another PEM file which contains only the RSA public key. This can be done by using the following command.

```
openssl rsa -in private-key.pem -pubout -out public-key.pem
```

Now, we generate self-signed certificates using the RSA private key by using the following command. The command will generate another PEM file which contains the certificate created by the secret key.

```
openssl req -new -x509 -key private-key.pem -out cert.pem -days 360
```

Now, we can create a pfx file which consists of certificate as well as secret key by using the following command. OpenSSL asks you to create a password to protect the file.

```
openssl pkcs12 -export -inkey private-key.pem -in cert.pem -out cert.pfx
```

After creating the certificate, with the help of the certificate we will sign the data and obtain the signature and server side validation is also done.

3 Proposed System

It is important to take into consideration the privacy and integrity of the data which is in transit. Here, the aim is to design a digital signature architecture that helps to enable the PKI services into the web applications. Integration of digital signature into web applications is not easy as there are many different signature representations and key storage formats. So here, we need to develop a standardised approach for the architecture to consume the underlying services. The proposed system enables

the user to perform a digital signature which is an electronic version using web extensions [11]. Along with the integrity of the data as well as authenticity, data is signed digitally, and a digital signature is being generated. The main objective of the proposed system is to have integrity and non-repudiation services into the web pages according to the user convenience, i.e. with a browser extension.

3.1 Methodology of Proposed System

Create a pfx certificate

Install the OPenSSL and webCrypto libraries and also npm modules

Write the code for the digital signature functionality.

Write the code for the browser extension development.

Integrate the code to load the extension onto the browser.

4 Browser Extension

Extensions are small software modules that facilitate and enhance browser experiences by customising the browser functionalities. These extensions are built on web technologies like HTML, CSS and JavaScript. We can modify the appearance of the web page by using chrome extensions. An extension can be built by different, but cohesive, components. These components include background scripts, content scripts, UI elements and options page. All the components may not be required for all the extensions. Requirement of the components depends on the functionality.

4.1 Integration of an Extension with Digital Signature Functionality

Implementation of the functionality of the digital signature is done through Java applets. The functionality takes input parameters as private key and the certificate [12]. The certificate is stored on the local storage as pfx file which is protected by a password in the case of linux. The certificate can be created in many ways. PKCS12 standard specifies the format of the digital certificate and it also allows to specify the path to the keystore, where certificate is stored. For compatibility of the digital signatures, we use the standards mentioned in the PKCS7. After all these, communication with browser is done through the JavaScript.

5 Conclusion and Future Work

Along with the security services such as confidentiality, authentication [13] and integrity services, non-repudiation also plays an important role in communication between customers and enterprises. The proposed digital signature architecture integrates non-repudiation services into web-based applications. With this architecture, an extension has been implemented such that it provides digital signature services to the web content selectively or entirely. The benefits of this method are

Digital signing will certainly become the future of the web

It will sign the web pages and prove the identity of one another.

The sender/receiver cannot deny their statements.

It also provides integrity services.

Here, we are implementing the extension for a specific browser (Chrome). In future, we can extend the work to all browsers which can be generic.

References

1. Ponnappalli HKB, Saxena A A digital signature architecture for web apps. Published by the IEEE Computer Society
2. Shailaja G, Phani Kumar K, Saxena A (2006) Universal designated multi verifier signature without random oracles. In: 2006 Proceedings—9th international conference on information technology, ICIT 2006, pp 168171
3. PKCS12: Personal information exchange syntax standard, RSA, 1999. <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.doc>
4. Pancholi VR, Bhadresh P, Hiran D (2018) A study on importance of digital signature for e-governance schemes. *Int J Innov Res Sci Technol* 4(10)
5. Kumar KP, Shailaja G, Kavitha A, Saxena A (2006) Mutual authentication and key agreement for GSM. In: 2006 international conference on mobile business, ICMB 2006, p 25
6. Wu W, Mu Y, Susilo W, Huang X (2009) Certificate-based signatures revisited 15(8):1659–1684
7. Patriciu V-V, Serb A (2000) Design aspects in a public key infrastructure for network applications security. In: Paper presented at the RTO IST symposium on “new information processing techniques for military systems” held in Istanbul, Turkey, 9–11 October 2000, and published in RTO MP-049
8. Huang Y, Chen F, Qu P Research on digital signature based on digital certificate. School of Information Engineering, Henan Institute of Science and Technology, Xinxiang, 453003, China
9. Haron GR, Daud NI, Mohamad MS (2018) Technology curve of digital signature on web browser. In: The 13th international conference for internet technology and secured transactions (ICITST 2018), University of Cambridge, United Kingdom
10. Wang Y Public-key cryptography standards: PKCS. University of North Carolina at Charlotte
11. Somé DF (2019) EmPoWeb: empowering web applications with browser extensions. In: 2019 IEEE symposium on security and privacy (SP), San Francisco, CA, USA, pp 227–245. <https://doi.org/10.1109/SP.2019.00058>
12. Haron GR, Daud NI, Mohamad MS (2019) Narrative of digital signature technology and moving forward. *Int J Intell Comput Res (IJICR)* 10(3)
13. Das ML, Saxena A, Phatak DB (2009) Algorithms and approaches of proxy signature: a survey. *Int J Netw Sec* 9(3):264–284

Design and Implementation of Cyber Threat Intelligence Data Mining Model



S. Lakshmi Narayanan, S. Shunmugavel, R. Prasanth, M. Satheesh Kumar, K. Srujan Raju, and K. Suthendran

Abstract These days, for every half seconds a cyber-attack is happening in this world. Most of them are hard to manage and mitigate by having appropriate cyber security measures. This article reports how cyber threat intelligence (CTI) can prevent an attack before it strikes, rather than researching about how to repair the damage caused by it. cyber threat intelligence in general refers to information that is collected from an open source or in an organization which mainly focuses on internal threat feeds such as antivirus and system logs. By gathering information about harmful threats earlier to an attack, organizations can develop enhanced CTI and thus protection of their infrastructure is possible. In addition, open threat exchange alien vault provides rich information about the threat data feeds which covers the day-to-day threats information is also considered. Here, an application programming interface is designed which fetches the relevant information from the open source The implementation of application programming interface and threat intelligence in Snort shall provide a greater security to our network and organization. The proposed work will keep organizations secure from the future threats as well.

Keywords Cyber threat intelligence · Snort · Threat data feeds

1 Introduction

Cyber threat intelligence is formulated on the circumstance, method, measure (indicator), logs, indication and taking actions on available or emerging threats to protect

S. Lakshmi Narayanan (✉) · S. Shunmugavel · R. Prasanth · M. Satheesh Kumar
Department of ECE, National Engineering College, Kovilpatti, India
e-mail: lakshminarayanansln28@gmail.com

K. Srujan Raju
Department of CSE, CMR Technical Campus, Hyderabad, Telangana, India

K. Suthendran
Department of IT, Kalasalingam Academy of Research and Education, Srivilliputhur, India
e-mail: k.suthendran@klu.ac.in

assets. It shows what is happening to an organization outside of its network, and therefore, what impact it will have on that company infrastructure. Some of the organizations are incorporating threat feeds into their network without having knowledge on additional data. This in turn complicates the analysis process. By choosing suitable tools, the process may be simplified and even threats can be prioritized. Our concept is gathering of basic information from available and future threats and utilizing other available open source intelligence, input from social media intelligence, individual intelligence, scientific intelligence and then analyses and filter out the data to produce different levels of threats and malicious actors based on their maliciousness, damage causing levels, data they target in an arranged report and this data feeds for automated security control system.

With a set of indication of compromise, it is possible to perform practical threat intelligence and exchanged between the known groups to enhance the organization's incident response and reform procedures. Gathered information is updated in a particular time interval to provide a better protection against threats. These data act as key mechanism which is feed in to Snort at a particular time interval and an API is developed to feed this data in Snort, where the API communicates with various top threat hunting and intelligence engines around the world. For information about emerging threats and threat actors, the API and the Snort are linked. So, the newly updated threat info is shared to the Snort and the network is protected against the emerging threat assets. Figure 1 represents the general block of a cyber threat intelligence.

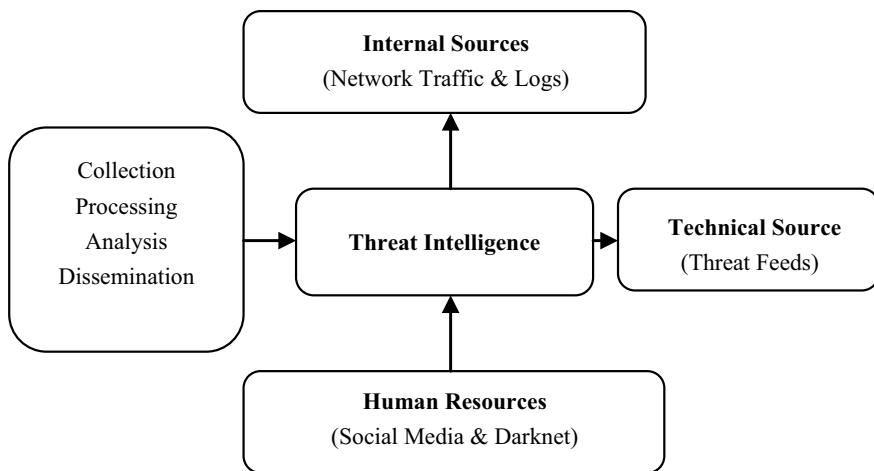


Fig. 1 General block model of cyber threat intelligence

2 Literature Survey

Threat intelligence is a prominent research area, where lots and lots of surveys and articles have been published. In this section, we briefly discuss about the articles and discuss the significance of our work.

Jisheng Wang et al. [1] proposed a system, where the local endpoint servers and clients are grouped into an entity and connected to centralized controller, which performs data analysis with certain IOCs, and malicious data is detected. Joseph et al. [2] proposed a scoring methodology in which threat information is combined, and normalized to improve quality, and each item is assigned with a threat score for categorization of these information based on type, maliciousness and confidence level. Eric Nunes et al. [3] searching the threat information not only in open source threat information platforms but also in dark and deep net sources and hacker forums for obtaining the information from the place of its origin. Giuseppe Settanni et al. [4] proposed word-based linking methodology, where for every work, TF and IDF are computed and words with IDF are ignored because it is considered as dictionary-based linking methodology, and they have engaged observed dictionary including ICT-security relevant words. The impact of cyber-attack on global economy is increasing year on year. In the year 2018, it resulted in \$445 billion loss [5]. Many companies rely on cyber threat intelligence to fix this problem. However, this is one that mitigates after an attack has occurred. Researchers have developed an intelligence to fix this problem with the help of various data on the internet.

Industry 4.0 is a combined version of IoT, CPS and smart X. The sensors used in it and the actuators are challenging to deal with when attacked [6]. To overcome this problem, they have developed a new capable intelligence. Thus, Industry4.0 is protected. Enhanced threat intelligence by collecting information from a harmful hacker advance to an attack so that the network can be better protected. As a proactive measure, researchers have detected mobile malwares with the help of neural network architectures and crated a threat intelligence [7].

In [8], TTPs are utilized to create an awareness to handle anomaly threats. If the data in a network is stolen, then the risks about it and the approaches to handle the resulting problems are studied in detail [9]. As per statistics of Symantec, the zero day weakness are increased to 125% in the year 2016 [10]. Furthermore, approximately 3/4th genuine websites have fixed vulnerabilities. The concept of grouping server and client into an entity may be tedious procedure and it requires a lot of data to be processed [11].

The scoring method can be known, and the threats actors can make stealthy ways to get pass the threshold rate. The information obtained from the dark and deep net should be trustworthy and it requires additional methods for checking the correctness of the obtained information. In every method, there is a possible way of passing over the barrier in the stealthy way and data is not fed back into the system, where the information is obtained. Moreover, establishing a formal and dedicated group for managing and maintaining threat intelligence activities [12]. The person in these groups should have an interest in analysis of threats and also have ideas of

making the threat analysis in an efficient way. Real-time analysis should take place by empowering SOC and enabling analysis [13].

There should be place for threat intelligence and attacker investigation in the yearly budget. It is the new way to the defence, and the organization can deal with the threat without being infected [14]. Threat intelligence sharing benefits every organization and helps in growth of business need and protection against information leakage through attacks. When one organization getting hit with a new malware or attack, other organizations who are likely to be hit next will ensure that they were able to detect and mitigate against the attack [15]. The threat intelligence gap is an opportunity for adversaries to attack, plunder the organization's data and pillage the cyber defence blind spot. According to recent surveys, nearly 80% organization believe in cyber threat intelligence that could help in cyber-attack prevention. But, 54% reviews that threat information is not timely. Organization is lacking confidence in cloud-managed security. The unknown objects on network and data changes within infrastructure should be monitored, real-time analysis, pc-to-pc intelligence, IP monitoring and reputation intelligence.

3 Analysis for Data Mining Model

3.1 Data Collection

The related work concentrates mostly on the threat data collection, and it would be upright if the proposed work is based on automated data collection. Initially, we collected the information about the existing threat information and threat actors from the open source threat intelligence platforms. For example, AlienVault, Open Threat Exchange is a platform which gives the relative information about the existing and the newly updates threat information as illustrated in Figs. 2, 3 and 4.

3.2 API Implementation

With the help of an API, for collecting information about emerging malicious and threat actors from the open source threat intelligence and processing the obtained information as depicted in Figs. 5 and 6. With the help of an API, the updated threat feeds will be directly gathered to our organization. Thus, API helps for interlinking the open source intelligence and Snort.

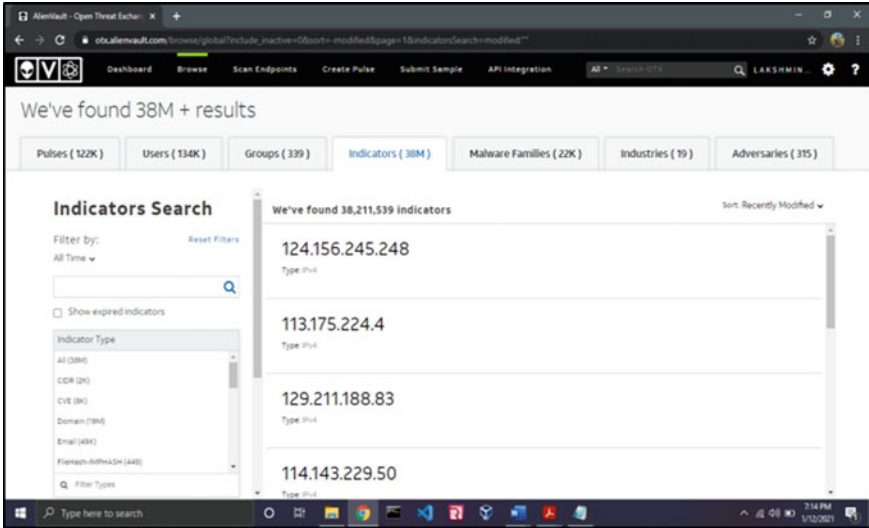


Fig. 2 Indicators

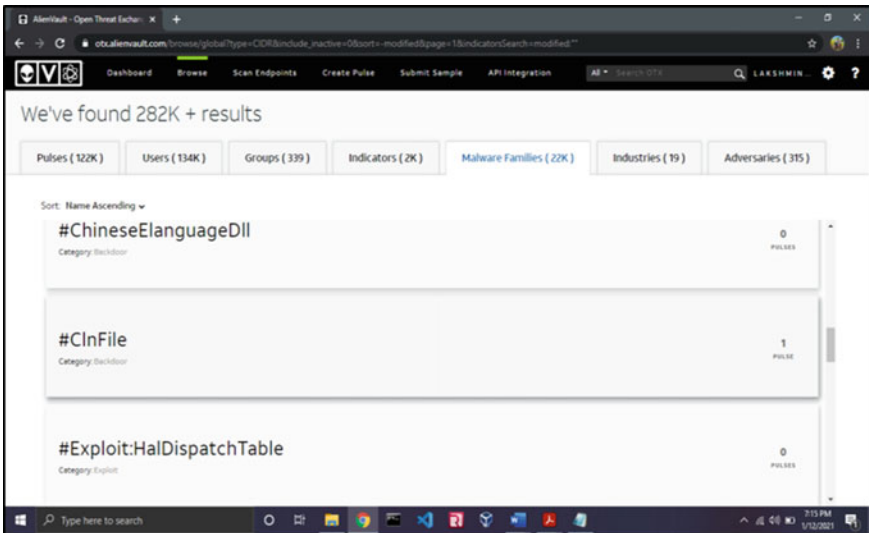


Fig. 3 Malware families

3.3 Integration with Snort

Snort will be fed with the threat intelligence data feeds through API integration. So that, the application will be cautioned with the emerging threats and threat actor

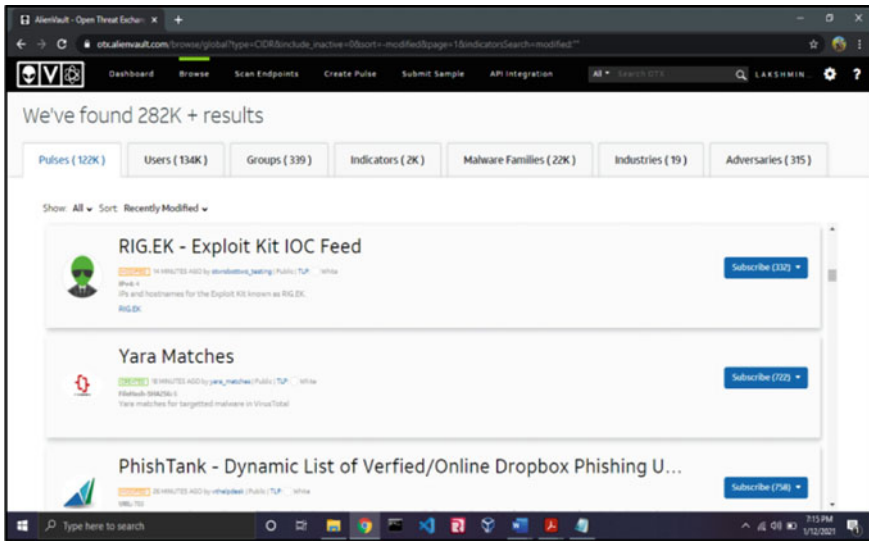


Fig. 4 Pulses

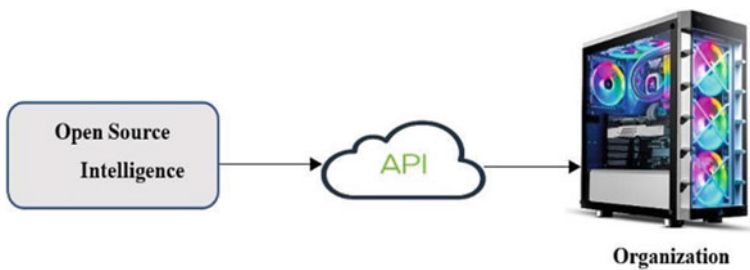


Fig. 5 API implementation

assets. Snort will be installed in the main server. So, the entire organization will be secured through the regular integration of threat data pulses through an API, and this pattern will be followed in the local client level PCs.

3.4 Blacklist

The integrated data feeds fed in the Snort and acts as a security wall. Therefore, when the user in the organization visits or browse on the Internet he/she may be kept protected from the adversaries, malwares, and the suspicious URL's. And how it works is that the IOCs in the Snort scans for the matches, when it matches while we browse in Internet then that suspicious file or URL will be blacklisted.

```
>>> otx.get_indicator_details_full(IndicatorTypes.DOMAIN,"textspeier.de")
{'general': {'indicator': 'textspeier.de', 'alexa': 'http://www.alexa.com/siteinfo/textspeier.de', 'whois': 'http://whois.domaint
t': 1, 'references': [], 'pulses': [{'indicator_type_counts': {'domain': 1}, 'pulse_source': 'web', 'TLP': 'white', 'description'
alware_families': [], 'is_modified': False, 'upvotes_count': 0, 'modified_text': '694 days ago', 'is_subscribing': None, 'refere
validator_count': 0, 'threat_hunter_scannable': False, 'is_author': False, 'adversary': '', 'id': '5b8b0b2a5c9bc06f886ce244', 'in
18-10-08107:45:46.839000', 'related_indicator_is_active': 1, 'threat_hunter_has_agents': 1, 'cloned_from': None, 'downvotes_count
': 0, 'indicator_count': 1, 'attack_ids': [], 'in_group': False, 'follower_count': 0, 'votes_count': 0, 'author': {'username': 'ky
lienvault.com/assets/images/default-avatar.png', 'is_following': False, 'id': '69607'}, 'related_indicator_type': 'domain', 'publ
scription': '', 'title': '', 'access_reason': '', 'access_type': 'public', 'content': '', 'type': 'domain', 'id': '1562169295'}, 'w
sive_dns', 'malware', 'whois', 'http_scans'}], 'geo': {'city_data': True, 'accuracy_radius': 1000, 'area_code': 0, 'continent_cod
ode': None, 'dma_code': 0, 'country_code': 'US', 'flag_url': '/assets/images/flags/us.png', 'asn': 'AS13335 CLOUDFLARENET', 'city
ngitude': -97.822, 'country_code3': 'USA', 'country_code2': 'US', 'latitude': 37.751, 'flag_title': 'United States of America'},
'https://api.otx.alienvault.com/api/v1/indicators/domain/textspeier.de/malware?page=2'], 'url_list': {'has_next': True, 'actual_
tp://www.textspeier.de/prada', 'hostname': 'www.textspeier.de', 'httpcode': 404, 'gsb': [], 'result': {'urlworker': {'ip': '104.2
', 'date': '2020-04-16T23:08:09', 'encoded': 'httpK3A/www.textspeier.de/prada'}, ('domain': 'textspeier.de', 'url': 'http://www.t
acke_3_in_1_padded_wandertag_9m1l8yyf', 'hostname': 'www.textspeier.de', 'httpcode': 404, 'gsb': [], 'result': {'urlworker': {'i
hes': []}}, 'date': '2020-04-16T23:08:09', 'encoded': 'httpK3A/www.textspeier.de/image/cache/data/category_13/adidas_damen_outdo
eier.de', 'url': 'http://www.textspeier.de/image/cache/data/category_30/scotch_soda_ralston_jeans_grey_hwfyxos9n', 'hostname': 'w
orker': {'ip': '104.27.162.228', 'http_code': 404}, 'safebrowsing': {'matches': []}}, 'date': '2020-04-16T23:08:09', 'encoded': '
soda_ralston_jeans_grey_hwfyxos9n'}, ('domain': 'textspeier.de', 'url': 'http://www.textspeier.de/image/cache/data/category_17/pr
y698537', 'hostname': 'www.textspeier.de', 'httpcode': 404, 'gsb': [], 'result': {'urlworker': {'ip': '104.27.162.228', 'httpcod
```

Fig. 6 Identified blacklisted pulses

3.5 Algorithm 1—Data Collection and Processing

Start

{

Input

 Activate open-source threat intelligence with API

 Collect threat feeds

Output

 Feed to Snort

Begin

 Import Indicator Types

 {

 Indicators = Hash Id for IOC in IOC's

 {

 shows "Type" (processing)

 }

 }

}

End

3.6 Algorithm 2—LICIT Prediction

Start

{

Input

Threat intel feeds

Output

Segregate

Legitimate or blacklisted.

Begin

1. Threat intel feed is collected

2. Browsed Logs (L_0, \dots, L_n) and files (F_1, \dots, F_n) are verified with the threat data feeds. (IOC's and Suspicious URL's).

3. Snort looks for any matches with the IOC's.

if ($F_0, \dots, F_n == \text{IOC}$)

{

The files (or) Suspicious URL is "blacklisted" and blocked

}

else

{

The file is legitimate.

}

}

End

4 Proposed Methodologies

To implement threat intelligence data mining model, the machine learning algorithm is used so that the system will learn about the threat intel feeds. First, the data is collected from various open source intelligence that gives the threat feeds such as IOCs, suspicious URL's, malware families, groups and adversaries as appeared out in Figs. 7 and 8. The above block diagram Fig. 9 will briefly give a clear idea about the working of this proposed methodology.

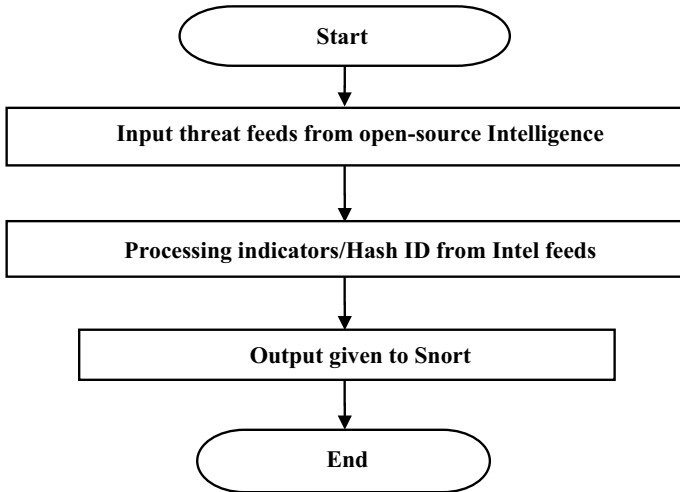


Fig. 7 Flow chart for data collection processing

The organizational user will interact in the Internet, the safety and security of the user is more important. The user may deal with the unknown files, there is always a possibility that the threat actors may affect the system and logs. So that, the threat intel feed from the open source intelligence is fed into the system Snort.

4.1 Experimental Setup

The experimental setup is arranged with two virtual machine, and Parrot 4.10 acts as an attacking machine and Kali 2021.1 acts as an IDS/IPS security wall as depicted in Fig. 10.

4.2 Rule Creation in SNORT

Snort is an open source intrusion prevention system (IPS) commonly used by most of the people in the world. The usage of Snort as follows: it can be used as a packet sniffer similar to TCP dump, and it is used as a packet logger which simplifies the network traffic debugging, it can also be used as an intrusion prevention system.

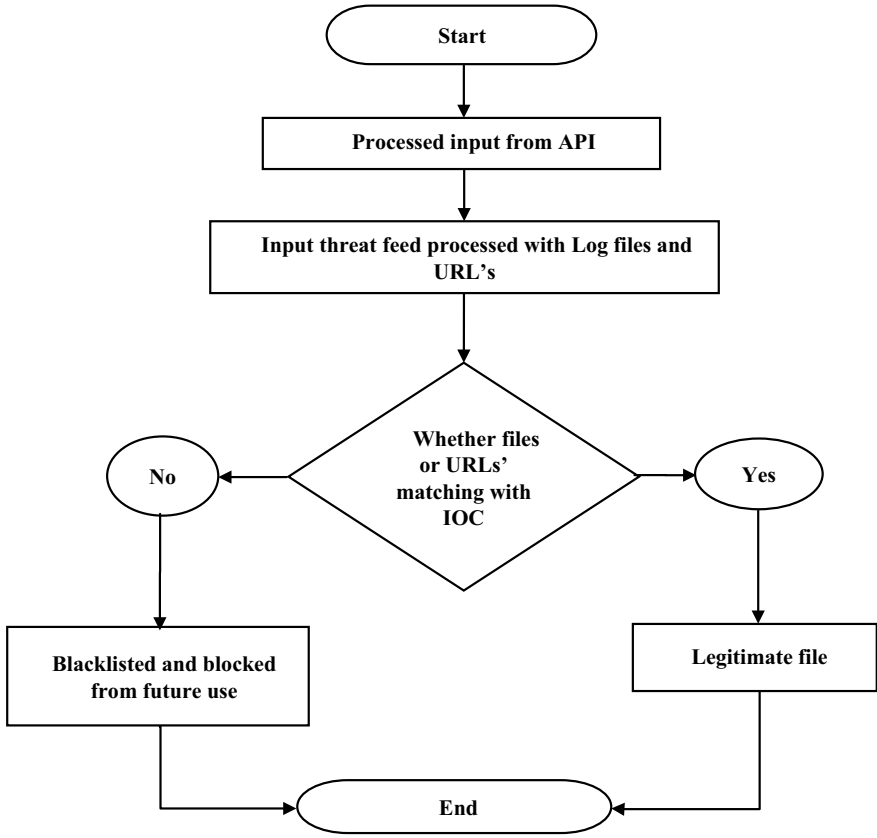


Fig. 8 Flow chart for licit prediction

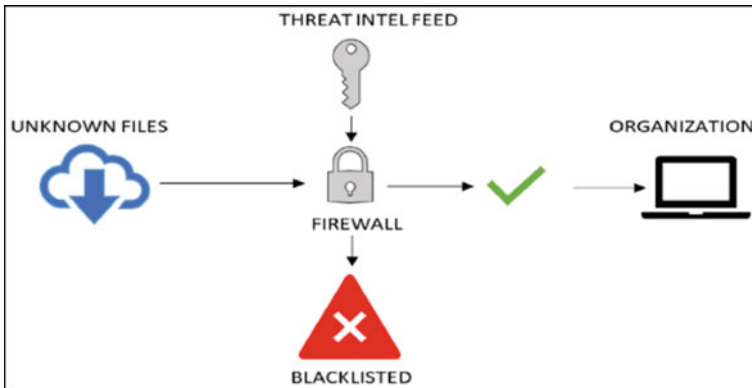


Fig. 9 Working model of threat intelligence data mining model

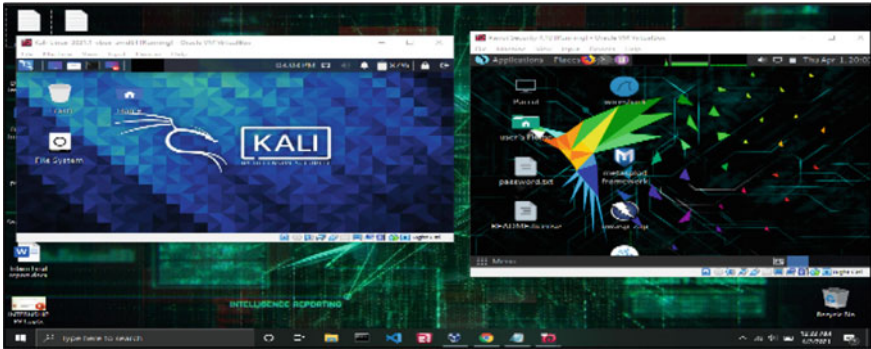


Fig. 10 Experimental setup

4.3 SNORT Rule Syntax

Snort as an intrusion detection system can be implemented with the rules framed as pictured below and as depicted in Figs. 11, 12 and 13.

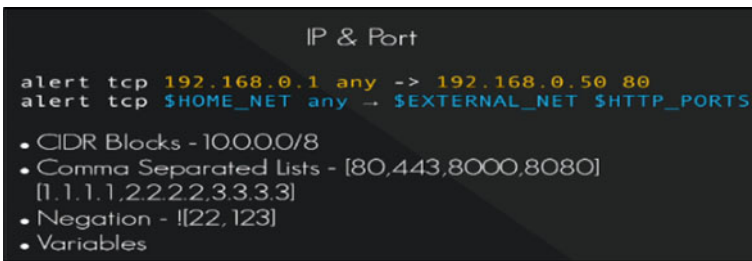


Fig. 11 IP address and port

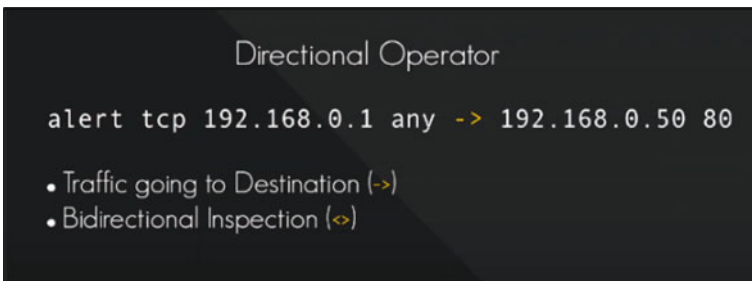


Fig. 12 Directional operator

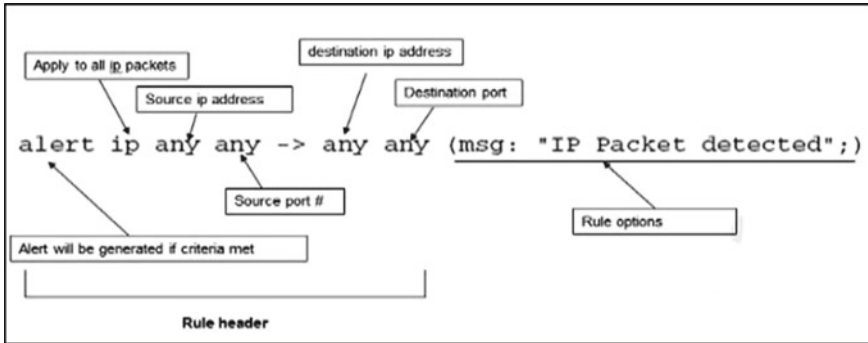


Fig. 13 Syntax

4.3.1 Header

Alert TCP 192.168.0.1 any -> 192.168.1.50 80

- Rule action
- Protocol
- Source IP/Port
- Direction
- Destination IP/Port

4.3.2 Rule Action

Alert TCP 192.168.0.1 any -> 192.168.1.50 80

- Alert
- Drop
- Pass
- Reject
- Drop

4.3.3 Protocol

Alert TCP 192.168.0.1 any -> 192.168.1.50 80

- TCP
- UDP
- ICMP
- IP

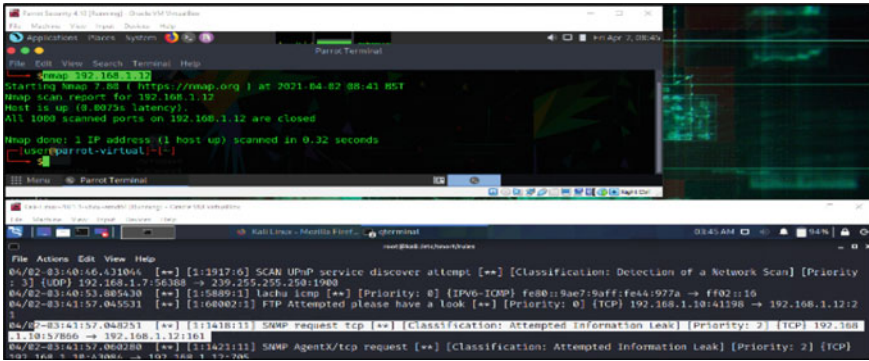


Fig. 14 Port scan from Parrot and detected in Kali (IDS)

4.3.4 Outcome

At first, pinging the host from VM, and then, VM from host to make sure whether all the setup is correct.

Custom Rules

In order to make use of the Snort efficiently and effectively, written the custom rules as per our use in the rules configuration of Snort.

Validation Running of the Custom Rules

Before running the Snort console, at first need to check if there anything erroneous. After this process, the Snort will be ready for the operation.

Reconnaissance from Parrot to Kali

The experimental setup is framed, performing a port scan from Parrot to Kali and the Kali which acts as a security wall that detects the reconnaissance and generates alert, also shows from which IP the attack is induced. Also, can see the word “Lachu icmp” in Fig. 14, which notifies that someone tries to ping the system, this is the custom rule and notification written by us in order to raise an alert for ping. Similarly, for the other port like FTP, SSH custom rule is written, in case any machine tries to reach the SSH or FTP or any ports this security wall can detect, alert and drop the request based on our use. For example, in Fig. 15, there is an FTP attempt from Parrot and Kali detected that with a custom rule and notification displays “FTP Attempted Please have a look”.

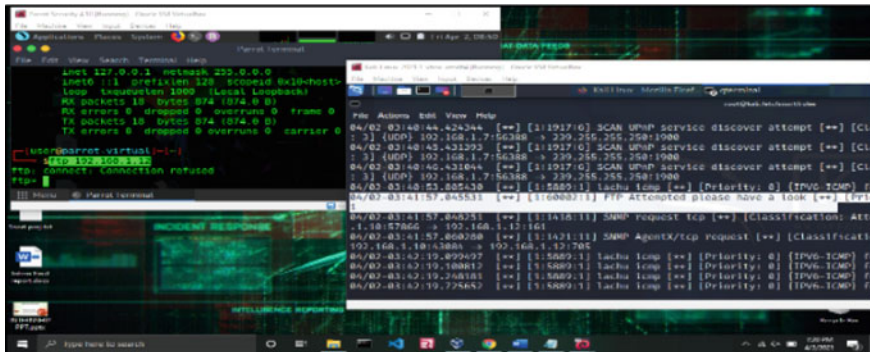


Fig. 15 FTP scan from Parrot to Kali

5 Conclusion

The implementation of intelligence in Snort provides the organizational greater security and system does not need to rely on the external tools for intelligence, which may be vulnerable, gives full access to the server admin. Although, our implementation of intelligence varies notably that covers fatal to extremely scientific. However, most of them use two key themes. At first, intelligence framework which offers detailed information on the real risks the organization faces. Furthermore, intelligence supports effective utilization of human resources to handle this process. Most of the security professionals agree that there is no 100% secure system. With the support of cyber threat intelligence, the enterprise network can be safeguarded. The implementation results show that the developed application interface can safeguard the network from attacks.

References

1. Wang J, Shen M-Y, Palkar P, Ramachandran S (2019) Collaborative and adaptive threat intelligence for computer security. US Patent, No.: US 10,469,514 B2
2. Magee JC, Andrews AM, Nicholson MW, James JL, Li HC, Stevenson CL, Lathrop J (2014) Collective threat intelligence gathering system. US Patent, No.: US 8,813,228 B2
3. Nunes E, Diab A, Gunn A, Marin E, Mishra V, Paliath V, Shakarian J, Thart A, Shakarian P (2016) Darknet and deep-net mining for proactive cybersecurity threat intelligence. In: IEEE conference on intelligence and security informatics, pp 7–12. <https://doi.org/10.1109/ISI.2016.7745435>
4. Settanni G, Shovgenya Y, Skopik F, Graf R, Markus (2017) Acquiring cyber threat intelligence through security information correlation. In: IEEE international conference on cybernetics, Exeter, United Kingdom
5. Samtani S, Chinn R, Chen H, Nunamaker Jr JF (2017) A new threat intelligence scheme for safeguarding industry 4.0 systems. *J Manage Inform Syst* 34(4):1023–1053. <https://doi.org/10.1080/07421222.2017.1394049>

6. Moustafa N, Adi E, Turnbull B, Hu J (2018) A new threat intelligence scheme for safeguarding industry 4.0 systems. *IEEE Access* 6(1):32910–32924
7. Samtani S, Grisham J, Patton M, Chen H (2017) Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence. In: *IEEE international conference on intelligence and security informatics, ISI*
8. <https://cupdf.com/document/cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.html>
9. Stoolman MA (2018) The cause of action for breach of data? The problem with relying on courts when managing the risks of cloud services, pp 1–26
10. <https://integracon.com/symantecs-2016-internet-security-threat-report/>
11. Bromiley M (2016) Threat intelligence: what it is, and how to use it effectively, a SANS review. <https://www.sans.org/webcasts/threat-intelligence-is-effectively-102622/>
12. Benjamin V, Chen H (2012) Securing cyberspace identifying key actors in hacker communities. In: *2012 IEEE international conference on intelligence and security informatics*. <https://doi.org/10.1109/ISI.2012.6283296>
13. Marsden T, Moustafa N, Sitnikova E, Creech G Probability risk identification based intrusion detection system for SCADA systems. <https://arxiv.org/abs/1711.02826>
14. Shreenivas D, Raza S, Voigt T (2017) Intrusion detection in the RPL connected 6LoWPAN networks. In: *Proceedings of 3rd ACM international workshop IoT privacy, trust, secure*, pp 31–38
15. Petersen R (2015) Data mining for network intrusion detection: a comparison of data mining algorithms and an analysis of relevant features for detecting cyber-attacks. Ph.D. dissertation, Department of Information Systems and Technology, Mid Sweden University, Sundsvall, Sweden

Gameplay Cognitive Decision Support Using Statistical and Non-statistical Parametric Fusion



K. Srujan Raju, Vinayak Jagtap, Parag Kulkarni, and M. Varaprasad Rao

Abstract Surprises are an inevitable part of any gaming application. These surprises eventually make decision-making a tough task. Cognitive learning always works in actions and associative responses. Gaming and cognition have a close association while decision-making in gaming or economics applications. These applications always respond to opponents' moves using statistical variants. These responses are always affected due to surprises. These surprises contribute to increasing uncertainty in decision-making. These surprises are not quantified and considered before action or response selection. This research is focusing on hypotheses as using non-statistical information such surprises can be optimized. There is also a need to associate quantified surprises and associated statistical variants. Here the model is proposed using data fusion techniques to use statistical and non-statistical parameters. This intern improves cognitive decision-making. The system can be adapted to other applications like gamification, economics applications, etc.

Keywords Surprises · Uncertainty · Non-statistical · Statistical parameter · Cognition · Gaming

1 Introduction

Cognitive computing is part of artificial intelligence and signal processing. Cognition has dictionary meaning as “A process by which build knowledge and understanding developed in mind” [1]. Humans are intelligent organism due to ability to learn

K. Srujan Raju (✉) · M. Varaprasad Rao
Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, India
e-mail: ksrujanraju@gmail.com

V. Jagtap
Department of Computer Engineering and Information Technology, College of Engineering,
Pune, India

P. Kulkarni
iKnowlation Research Labs Pvt. Ltd, Pune, India

from the environment. This learning is in the form of building knowledge around problems. There might be common knowledge used to solve multiple problems, but each problem has a different problem space and knowledge space. These spaces are defining context which can be used in solving these problems separately. The context of the problem helps to decide information and relevant knowledge building needed in decision-making. This intern depicts problem space and knowledge space [2, 3].

Currently, many problems are solved by formulating them in gaming scenarios which are called gamification. It is the branch of computation that helps to model problems in-game with different aspects as game decision, problem-solving with gamification, etc. This problem formulation in the game has different analogies like affinity in decision support or business is defined with brand loyalty, etc. The dynamic problems have a lot of uncertainty similar to gaming scenarios. Hence, gamification helps to understand constraints, dependencies, and surprises before solving problems in the gaming domain. For example, finding the shortest path problem can be modeled as the game of a puzzle. This modeling might associate statistical data association like backtrack is the penalty in the game [4, 5].

Gaming and cognition have a very close association, cognition is developed for problem-solving similar to gaming problems [6]. Cai et al. have defined cognitive gaming for this fusion [7, 8]. Hence, gaming application helps to develop learning models for cognitive problem-solving. Many gaming applications have short-term and long-term knowledge vectors which may help in decision-making in the case of cognitive problem-solving. For example, a game of Tic-Tac-Toe helps to understand the position and associated weights of each move. In real life, cognitive problems are also similar which can be analyzed moves (self/opponents), associated impacts, projection, etc. [9, 10].

These cognitive knowledge building and understanding have information in various forms this information. Here mainly considered statistical and non-statistical. Due to the variety of such information, much recent computing system has dependencies while building knowledge to map exact contextual information. These computational systems unable to associate contextual information derived from statistical and non-statistical data. This is due to uncertainty associated with and surprises coming in dynamic systems. In this paper, a generic system is proposed in the case of gaming decision-making using cognitive science. The proposed system focuses to understand and apply contextual information by associating and fusing data from problem space.

2 Literature Survey

Cognitive computing has a variety of applications from real life like natural language processing (NLP), speech, vision processing, and identification. To solve such a problem, a theory proposed has imitating nature to human problem-solving. Some researchers used the human brain and nervous system imitation which is called artificial neural network (ANN). This intern-designed cognitive system strives from

human-centric data analysis to adaptive nature [1–3]. Cognitive computing has mainly comprised of four features:

- a. Adaptive
- b. Interactive
- c. Stateful
- d. Contextual

The cognitive applications currently used to have two different types of analysis namely adaptive and natural language interactions. These analyses are used separately for problem-solving. This is the reason which has dependencies while making the decision. The statistical and natural language association and fusion might help in improving decision support. The chatbots and other mechanisms designed to solve queries based on NLP processing but miss statistical analysis of the query asked. The queries and associated responses might have better results if there is a statistical and non-statistical parametric fusion [6–8].

Multiple answers are emerging for the different scenarios which make decision-making a hard task. Selecting the most appropriate decision from the list needs a trade-off between different variants. This trade-off needs intelligence with fast with correctness. This can be achieved with gaming platform analogies and modeling. This information processing needs expert analysis for selecting the most appropriate answer [9, 10].

Many economical problems have constraints and associated information in various forms. These problems can be modeled easily with gamification. Such problems are highly dynamic and cost a lot of wrong decisions. These decisions henceforth need a precise domain associated context and strong statistical support [11, 12]. In machine learning and artificial intelligence, it is always believed that more and more information improves accuracy. But recent intelligence systems focusing on contextual decision-making rather than rule-based or pattern-based machine learning [13, 14].

Missing contextual information always invites uncertainty and surprises. The uncertainty in the form of lack of information or uneven distribution of data and non-associated decision-making. This intern results from more confusion in decision-making. Modeling uncertainty for contextual aware systems helps in decision support. Many researchers have proposed different approaches to model uncertainties like probabilistic [15–18].

To summarize, there is a need to build a cognitive system that uses the statistical and non-statistical data for deriving the right context in decision-making under surprises and uncertainties. The proposed system is proposed for cognitive information processing which uses statistical and non-statistical data to understand problem space, uncertainties, and surprises associated. The proposed system uses this information to build knowledge used in decision support.

3 Proposed System

Figure 1 represents the proposed system; the system comprises multiple information classified in statistical and non-statistical. The information proposed for building knowledge and together used in decision-making. To use non-statistical data, the natural language interaction is used for information capturing which intern converted to knowledge. For example, the stock prices of a company are forecasted to be raised, but unfortunately, natural disasters, emergencies, or government policies may affect this forecasting. The current situation like the COVID-19 pandemic might affect such forecasting. Here statistical data, parameters, features are forecasting trends for an increase in stock price. But environmental factors mentioned above are contributing to price fall. These events are dynamic and can impact business severely. A simple NLP-based application can help us to understand this trend change from news/commentary or other data. These are non-statistical parameters that can be used after NLP. NLP processing can capture contextual surprises and uncertainty which is missing in statistical parameters. But the question remains how to use these non-statistical and statistical parameters together. For that, different data fusion techniques are used here like joint probability fusion as given below:

$$P(\lambda|Z) = C^{-1} \prod_{j \in \lambda} (P((\lambda(j)|Z(j)))^{\alpha(j)} \prod_{\tau \in \lambda} (L(\tau|Z))$$

where P is probability with C is constant and L is likelihood function (Fig. 2).

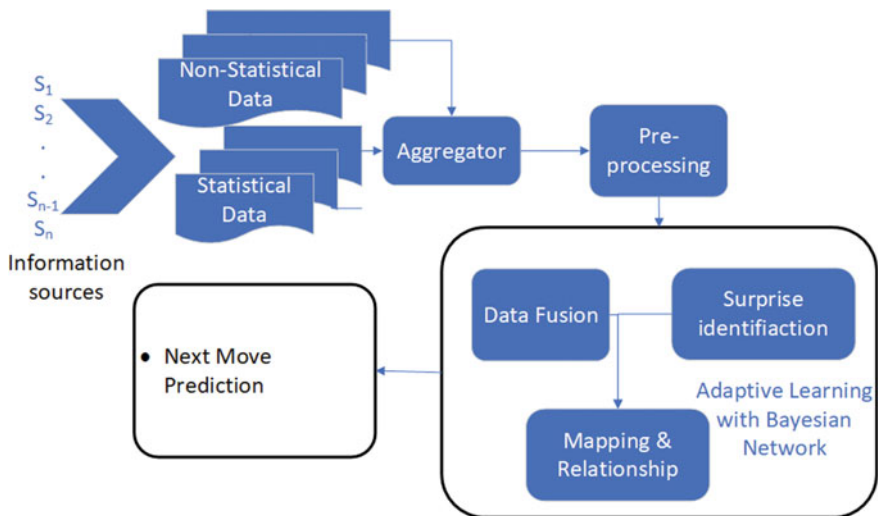


Fig. 1 Proposed system

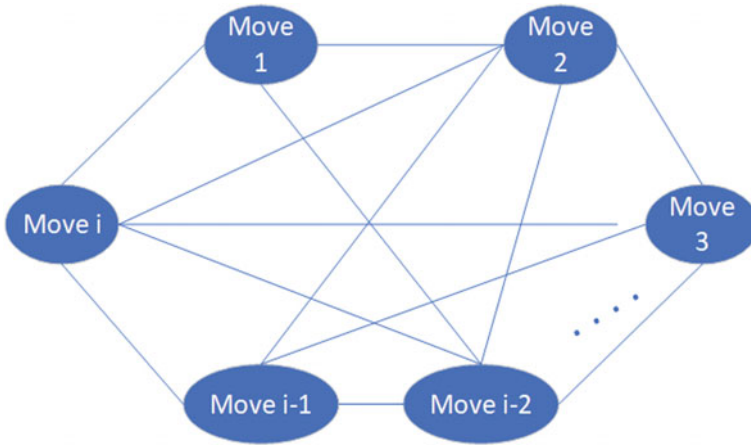


Fig. 2 Sample Bayesian network

Table 1 Stock commentary/news and impact

ID	Commentary/news articles	Impact indices
1	BPCL Cuts Refinery Throughput as Lockdowns Hit Fuel Demand	-0.3
2	Why BPCL Doesn't Plan To Sell Stake In Indraprastha Gas, Petronet LNG	-0.7

4 Results and Discussion

Stock data with news are used for experimentation for statistical and non-statistical operations from the stock website (<https://www.bloombergquint.com/markets>). These stock prices are modeled as gaming applications where profit should be more. An adaptive learning-based Bayesian network is used stock prices between different stocks to determine price drop or rise. This Bayesian network is designed for multi-players selling and purchasing stock and associated price change. The results show that the accuracy of prediction is increased for the proposed system. Table 1 represents non-statistical processing performed on stock price commentary. Figure 3 represents the accuracy results comparison.

5 Conclusion

Cognitive computing needs adaptive learning as well as the support of multiple information while building knowledge. The statistical and non-statistical data together generate more precise and contextual information for building knowledge. Modeling uncertainties in gaming for stock data makes focused adaptive learning in the context

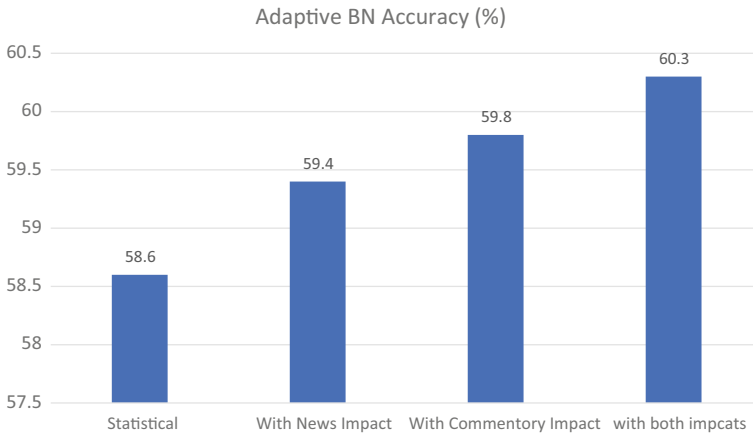


Fig. 3 Accuracy comparison

of stock prices. This intern improves the performance of decision-making. This system can be extended with multiple information sources processed together.

References

1. Modha DS, Ananthanarayanan R, Esser SK, Ndirango A, Sherbondy AJ, Singh R (2011) Cognitive computing. *Commun ACM* 54(8):62–71
2. Chen M, Herrera F, Hwang K (2018) Cognitive computing: architecture, technologies, and intelligent applications. *IEEE Access* 6:19774–19783
3. Noor AK (2014) Potential of cognitive computing and cognitive systems. *Open Eng* 5(1)
4. Zichermann G, Cunningham C (2011) *Gamification by design: implementing game mechanics in web and mobile apps*. O’Reilly Media, Inc
5. Fuchs M, Fizek S, Ruffino P, Schrape N (2014) *Rethinking gamification*. Meson Press
6. Demirkan H, Earley S, Harmon RR (2017) Cognitive computing. *IT Prof* 19(4):16–20
7. Cai W, Chen M, Leung VCM (2014) Toward gaming as a service. *IEEE Internet Comput* 18(3):12–18
8. Cai W, Chi Y, Leung VCM (2017) Cognitive gaming. *IT Prof* 19(4):55–62
9. Harrell DF (2009) Computational and cognitive infrastructures of stigma: empowering identity in social computing and gaming. In: *Proceedings of the seventh ACM conference on creativity and cognition*, pp 49–58
10. Stapleton D War gaming supported by cognitive computing and time manipulation
11. Angelelli L, Stapleton D (2015) Cognitive computing and serious gaming—providing superior strategic planning to stabilize world water resources for the future human race
12. Cai W, Chan HC, Wang X, Leung VC (2015) Cognitive resource optimization for the decomposed cloud gaming platform. *IEEE Trans Circuits Syst Video Technol* 25(12):2038–2051
13. Sung H-Y, Hwang G-J, Yen Y-F (2015) Development of a contextual decision-making game for improving students’ learning performance in a health education course. *Comput Educ* 82:179–190
14. Hambrick DC, Snow CC (1997) A contextual model of strategic decision making in organizations. *Acad Manage Proc* 1977(1):109–112. Briarcliff Manor, NY 10510

15. Antifakos S, Schwaninger A, Schiele B (2004) Evaluating the effects of displaying uncertainty in context-aware applications. In: International conference on ubiquitous computing. Springer, Berlin, Heidelberg, pp 54–69
16. Ye J, McKeever S, Coyle L, Neely S, Dobson S (2008) Resolving uncertainty in context integration and abstraction: context integration and abstraction. In: Proceedings of the 5th international conference on pervasive services, pp 131–140
17. Truong BA, Lee Y-K, Lee S-Y (2005) Modeling and reasoning about uncertainty in context-aware systems. In: IEEE international conference on e-business engineering (ICEBE'05). IEEE, pp 102–109
18. Huettel SA, Song AW, McCarthy G (2005) Decisions under uncertainty: probabilistic context influences activation of prefrontal and parietal cortices. *J Neurosci* 25(13):3304–3311

Securing Communication in IoT Environment Using Lightweight Key Generation-Assisted Homomorphic Authenticated Encryption



Ajeet Singh, Vikas Tiwari, Appala Naidu Tentu, and Ashutosh Saxena

Abstract Cryptographic key establishment is an essential component between any pairwise resource-constrained sensor nodes inside an Internet of Things (IoT) infrastructure. Keeping in mind that IoT devices are computationally limited and resource constrained, it is important that the primitives employed in the construction of any key generation mechanism are lightweight. During communication among IoT sensor nodes/ smart devices, data privacy preservation is a major challenge to handle. In this paper, we propose an oracle for securing communication in IoT environment using lightweight key generation-assisted homomorphic authenticated encryption. In order to judge its efficiency and adaptability, we carried out the computational complexity, security, correctness analysis and experimental evaluation of the developed framework. Later, the comparative analysis is also performed with some significant state-of-the-art approaches.

Keywords Key management · Security · IoT · Authentication · Key management centre · Homomorphic computations

1 Introduction

With the Internet of Things (IoT) predicted to connect approx 29 billion devices by the end of 2022, securing these particular connected appliances is surely a big security concern [1]. Security is a term that is used to encompass the notions such as integrity, confidentiality and privacy that typically are achieved utilizing crypto-

A. Singh (✉) · V. Tiwari
Acharya Nagarajuna University, Guntur, AP 522510, India
e-mail: ajeets@uohyd.ac.in

A. Singh · V. Tiwari · A. N. Tentu · A. Saxena
C.R. Rao Advanced Institute of Mathematics, Statistics and Computer Science, UoH Campus,
Prof. CR Rao Road, Hyderabad, Telangana 500046, India

A. Saxena
CMR Technical Campus, Hyderabad, Telangana 501401, India

graphic encryption procedures [2, 3]. Establishing and supervising a group key in a particular IoT environments, where the involved devices are resource constrained, battery-powered, as well as the groups [4] are dynamic by computational nature, which is certainly a non-trivial problem. During the communication among IoT sensor nodes/ smart devices, data privacy preservation is a major challenge to handle. During communication among IoT sensor nodes/ smart devices, data privacy preservation is a major challenge to handle. Homomorphic encryption [5] is one of the most feasible and compatible method to exploit in this scenario. In the field of abstract algebra, homomorphism can be defined as—mapping that preserves all the algebraic structures between domain and the range of an algebraic set.

1.1 Organization of the Paper

Rest of this paper is organized as: Sect. 2 presents the summary of prior works done in this domain over the past years. Our proposed framework/ oracle is presented in Sect. 3. Section 4 presents empirical analysis of the proposed oracle. Experimental evaluation and obtained results along with the comparisons with different schemes are presented in Sect. 5. Finally, Sect. 6 presents the conclusive summary of this paper.

2 Related Work

A matrix-based key establishment scheme without the secret sharing consideration is presented in [2]. Mesmoudi et al. [3] proposed an smart and dynamic key management prototype for the hierarchical wireless sensor networks. Chen et al. in [6] developed a secure light weight network coding pseudonym scheme. This developed scheme can defend against insider as well as outsider adversarial attackers. Authors in [7] have proposed efficient linearly homomorphic authenticated encryption method. Nafi et al. [8] Given a lightweight key establishment protocol for IoT sensor nodes exploiting matrix-based primitives. Singh et al. [9] have given a scheme for pairwise key agreement with updation of key pre-distribution private shares while new nodes are being added to the MANET. Zhang et al. [10] given an authenticated key agreement scheme using one-way hash functions. Gebremichael et al., in their work [4], implemented a computationally secure and lightweight group key establishment protocol appropriate for resource-constrained IoT nodes.

3 Proposed Framework

The adopted framework along with the detailed algorithmic procedure steps is given in this section. Summary of notations used is provided in Table 1.

3.1 Authentication

Consider S_i is the i -th registered sensor node in the communication ecosystem. The steps in this authentication phase are as follows:

1. Each $S' \in \text{set of } S_i^s$ inputs their $\{I, P\}$, then mobile computes $SID = SID^m \oplus h(I||P)$, $a_i = a_i^m \oplus h(I||P)$. Next, it randomly selects the 140-bit number $\theta \in Z_n^*$ & current time-stamp T . Finally, it sends auth_req message ($msg_1, msg_2, msg_3, msg_4$) to CS via public channel.

$$\begin{aligned} msg_1 &= h(SID_s||T) \oplus SID_i \\ msg_2 &= h(SID_i||SID_s||a_i) \oplus \theta \\ msg_3 &= h(SID_i||SID_s||a_i||\theta) \oplus SID_j \\ msg_4 &= h(SID_i||SID_j||SID_s||a_i||\theta) \end{aligned}$$

2. After receiving (msg_1, msg_2, msg_3 and msg_4) from each S' , CS checks validation of time as $\mathbb{T} - T \leq \delta$, where δ is max time threshold for acceptance of messages and \mathbb{T} is depicting the current time obtained message. If it's true \Rightarrow (goes towards the next phase), else \Rightarrow (CS rejects authentication request).

3.2 Key and Other Parameters Generation

1. KMC Generates 'a'.
2. KMC chooses $\mathcal{K} [] []$ as random orthogonal matrix of dimension 'n' using sub-procedure given below

Table 1 Summary of notations

Notation	Description
KMC	Key management centre
CS	Cloud server
$\{I, P\}$	Identity and password for individual sensor node
\mathcal{K}	Key for IoT communication system
S_i	i^{th} registered sensor node
h	One-way hash function
T	Current time-stamp
θ	Randomly generated 140-bit number

2(a): Use recursive definition for $\mathcal{K}^{(n)}$, starting with $\mathcal{K}^{(1)} = [1]$ as

$$\mathcal{K}^{(2n)} = \begin{bmatrix} \mathcal{K}^{(n)} c_n & -\mathcal{K}^{(n)} s_n \\ \widehat{\mathcal{K}}^{(n)} s_n & \widehat{\mathcal{K}}^{(n)} c_n \end{bmatrix}$$

where, $\widehat{\mathcal{K}}^{(n)}$ has some form as $\mathcal{K}^{(n)}$ except that the c_i and s_i indices are all increased by n .

2(b): Use the following formula to determine the (i, j) entry, $(\mathcal{K}^{(n)})_{i,j}$, in $\mathcal{K}^{(n)}$:

$$(\mathcal{K}^{(n)})_{i,j} = \prod_{r=1}^k t_{i_r} (\theta_{2^r} \lfloor \frac{i-1}{2^r} \rfloor + 2^{(r-1)} + j_r \frac{\pi}{2})$$

where,

$$i-1 = i_1 + 2i_2 + \dots + 2^{(k-1)}i_k$$

$$j-1 = j_1 + 2j_2 + \dots + 2^{(k-1)}j_k$$

the i_r 's and j_r 's are 0 (or) 1, $t_0(\theta) = \cos(\theta)$ & $t_1(\theta) = \sin(\theta)$

3. KMC sends generated parameters 'a' and $\mathcal{K}[\]$ to IoT sensor node over the secure channel.

3.3 IoT Sensor Node Side Computation

1. Generates two equal size sets S_1 and S_2 having elements as random primes, where each set consists of 'a' number of elements

$$S_1 = X_1, X_2, X_3, \dots, X_a$$

$$S_2 = Y_1, Y_2, Y_3, \dots, Y_a$$

2. Compute $n_1 \leftarrow X_1 \times Y_1, n_2 \leftarrow X_2 \times Y_2, \dots, n_a \leftarrow X_a \times Y_a$

$$S = \prod_{i=1}^a n_i$$

3. Calculate transpose of orthogonal matrix \mathcal{K} as \mathcal{K}^T

$$\mathcal{K}^T \leftarrow \text{Transpose}(\mathcal{K}) \bmod \mathbb{Z}_S$$

4. Node provides input as \mathcal{M} ranges from 1 to S .
5. Node generates \mathbb{R} ranges from 1 to S such that $\mathbb{R} \neq \mathcal{M}$.
6. Create matrix Y of dimension $[a \times (n-1)]$, such that each row comprises only single event of \mathcal{M} and remaining $(n-2)$ occurrences of \mathbb{R} .
7. Apply Chinese Remainder Theorem (CRT) to obtain the solutions $(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{(n-1)})$ of corresponding simultaneous equations as follows:

$$\begin{aligned}
Y_{11} \bmod n_1 &= \alpha_1, Y_{12} \bmod n_1 = \alpha_2, \dots, Y_{1(n-1)} \bmod n_1 = \alpha_{(n-1)} \\
Y_{21} \bmod n_2 &= \alpha_1, Y_{22} \bmod n_2 = \alpha_2, \dots, Y_{2(n-1)} \bmod n_2 = \alpha_{(n-1)} \\
&\vdots \\
Y_{a1} \bmod n_a &= \alpha_1, Y_{a2} \bmod n_a = \alpha_2, \dots, Y_{a(n-1)} \bmod n_a = \alpha_{(n-1)}
\end{aligned}$$

8. Node encrypts input data \mathcal{M}_i as:-

$C_{i_MAT} \leftarrow \mathcal{K}^T \times D[\mathcal{M}_i, \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{n-1}] \times \mathcal{K}$, where D represents diagonal matrix of dimension $n \times n$ with diagonal elements as $\mathcal{M}_i, \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{n-1}$ and remaining elements are zeros.

9. Node outsources the encrypted data C_{i_MAT} to the cloud server for computation.

3.4 Computation on Encrypted Data

1. Perform homomorphic computation on received encrypted data from sensor node.
2. Circuit computation for encrypted data C_{i_MAT} upto optimal depth.
3. Sends back the computed results to sensor node.

3.5 Decryption Circuit Evaluation

Sensor node decrypts the computed result as

$$P_{i_MAT} \leftarrow \mathcal{K} \times C_{i_MAT} \times \mathcal{K}^T$$

$$\text{Do, } \psi_i \leftarrow P_{i_MAT[1][1]}$$

if ($\psi_i == \mathcal{M}_i$)

Results Verified.

4 Empirical Analysis of Proposed Oracle

4.1 Computational Complexity Analysis

Subprocedure 3.2 takes $O(\log(n)n^2)$ time complexity, where n is dimension of the random orthogonal matrix.

Subprocedure 3.3 (step 4) takes $O(n^2)$ time in computation.

Subprocedure 3.3 (step 7) involves to take a system of t congruences of form $x \equiv a_i \pmod{n_i}$ and carrying out certain computations to obtain all the solutions which are in form

$$x \equiv \sum_{i=1}^t a_i \frac{\mathbb{N}}{n_i} \left[\left(\frac{\mathbb{N}}{n_i} \right)^{-1} \right]_{n_i} \pmod{\mathbb{N}}, \text{ where } \mathbb{N} = \prod_{i=1}^t n_i \quad (1)$$

Thus, (I) involves amortized cost of $O(\text{len}(\mathbb{N})^2)$.

Subprocedure 3.3 (step 8) and 3.5 consist of mainly matrix multiplication which requires essentially cubic number of operations, i.e. runs in $O(n^3)$ time. Though, there is a possibility to follow procedure [11] with an improved amortized complexity bound as $O(n^{2.373})$; however, for some higher tensor powers [12], the complexity bound obtained was $\approx O(n^{2.5621})$.

4.2 Security and Correctness Analysis

The plaintext \mathcal{M} is getting encrypted with the generated key \mathcal{K} . Any query comes from IoT sensor node side privately at cloud server such that the cloud responds on requests (i.e. carry out scientific computations on outsourced query parameters) without any intention to know them. The proposed method has ability to perform operations on encrypted data without decrypting them which solves the problem of confidentiality and privacy while communication in IoT infrastructure. We observe that,

Dec_Proc ($\mathcal{K}, \mathcal{K}^T, \mathcal{C}_i, S$)

$\mapsto \mathcal{K} \times \mathcal{C}_{i_MAT} \times \mathcal{K}^T$

$\mapsto \mathcal{K} \times \mathcal{K}^T \times D[\mathcal{M}_i, \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{n-1}] \times \mathcal{K} \times \mathcal{K}^T$

since, $\mathcal{K}^{-1} = \mathcal{K}^T$ i.e. $\mathcal{K} \cdot \mathcal{K}^T = \mathcal{K}^T \cdot \mathcal{K} = I$

$\mapsto I \times D[\mathcal{M}_i, \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{n-1}] \times I$

$\mapsto D[\mathcal{M}_i, \alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{n-1}]$

$\mapsto P_{i_MAT}$

do, $\psi_i \leftarrow P_{i_MAT[1][1]}$

$\psi_i == \mathcal{M}_i$

It validates the correctness of the proposed oracle.

5 Experimental Evaluation and Results Discussion

Our experimental set-up contains system environment as Ubuntu 16.04 LTS with 64 bit OS, 8 GB RAM, processor as Intel Core i7-860 @ 2.80 GHz clock speed.

Python (v3.5.2) installed and used for implementation. Results analysis is compiled in form of Tables 2 and 3. In Table 2, different parameter values for a and $\text{Dim}(\mathcal{K})$ are taken into consideration in each case. After executing proposed procedure, the correctness of the prototype functionality and Error% in decryption circuit is judged. In Table 3, Additive (+) and Multiplicative (\times) homomorphic properties are validated on different test cases.

Table 2 Experimental results on various test case scenarios

Scenario	a	Dim (K)	\mathcal{M}	\mathcal{C}	ψ	Is ($\psi = \mathcal{M}$)	Error %	Time (s)
1	5	4	356	1.005e+13	3.559e+02	Yes	0.001	0.0074
2	5	8	1472	3.3325e+15	1.472e+03	Yes	0.0	0.0125
3	5	16	1729	3.1916e+10	1.7289e+03	Yes	0.001	0.0361
4	6	31	2041	1.2235e+13	2.0410e+03	Yes	0.0	0.1034
5	6	33	91072	3.9984e+17	9.1035e+04	\simeq Yes	0.0037	0.1127
6	6	50	98721	2.59658e+17	9.8626e+04	\simeq Yes	0.0095	0.2041
7	5	127	316292	6.67912e+14	3.162919e+05	Yes	0.00001	0.4517

Table 3 Performance with reference to scheme correctness and homomorphic properties validation on test cases

Sr.	a	Dim (\mathcal{K})	$(\mathcal{M}_1, \mathcal{M}_2)$	$R_1 \leftarrow +_{(C_1, C_2)}$	$R_2 \leftarrow \times_{(C_1, C_2)}$	$D_{\mathcal{K}}(R_1)$	$D_{\mathcal{K}}(R_2)$	$\mathcal{E}(\%)$	HP
1	5	8	(3961, 249)	1.948e+12	5.7800e+24	4.2100e+03	9.8628e+05	0.0	+ , ×
2	5	8	(1726, 921)	1.718e+12	4.5360e+24	2.647000e+03	1.589612e+06	0.00002	+ , ×
3	5	16	(2369, 1499)	2.7390e+14	2.8886e+29	3.8681e+03	3.551123e+06	0.000008	+ , ×
4	5	16	(148, 985)	2.21313e+14	2.45924e+29	1.13297e+03	1.45780e+05	0.0	+ , ×

where denotions are as: $+_{(C_1, C_2)} \Rightarrow$ Homomorphic Addition of C_1 and C_2 , $\times_{(C_1, C_2)} \Rightarrow$ Homomorphic Multiplication of C_1 and C_2 , $D_{\mathcal{K}}(R_1) \Rightarrow$ Decryption of homomorphically computed result (R_1), $D_{\mathcal{K}}(R_2) \Rightarrow$ Decryption of homomorphically computed result (R_2), $\mathcal{E}(\%) \Rightarrow$ Decryption Circuit Error(%), HP \Rightarrow Homomorphic properties, (+, ×) \Rightarrow Additive and Multiplicative homomorphic property correspondingly

Table 4 Comparative analysis of schemes

Schemes	Authentication	Primitives used	Computation cost
Blom [13]	No	MDS codes	$O(N^3)$
Zhang et al. [14]	No	Matrix-based routines	$O(3N^3)$
Lukas M et al. [15]	Yes	Entropy source	$O(N \cdot \log_2 N)$
Gheisari et al. [16]	No	K-anonymity	$O(N^{2.6}) + O(2^\lambda)$
Nafi et al. [8]	Yes	Matrix-based routines	$O(N^2 + MAC)$
Our scheme	Yes	Abstract algebra, Homomorphism	$O(N^2) + O(\lambda^{7.1})$

5.1 Comparative Analysis

This section presents the benchmarking/ comparisons with some significant existing schemes for secure communication in IoT infrastructure.

In Table 4, N : is the size of problem input with respect to growth rate, MAC : represents message authentication code and λ : is the security parameter. Both, the resource requirements of the cryptographic algorithm (or protocol) as well as the adversary's probability of breaking security are expressed in terms of the security parameter.

6 Conclusion

With the eruptive surge of data produced by different sensor nodes in an IoT ecosystem, the conventional cloud computing strategies by outsourcing entire data to the cloud for computation and processing has moderately failed in order to meet the certain requirements such as: maintaining data privacy, resource-constrained nature, low storage cost and authentication during communication. During communication among IoT sensor nodes/ smart devices, data privacy preservation is a major challenge to handle. This paper proposes an oracle and validates in terms of experimental evaluation, performance and comparative analysis for securing communication in IoT environment using lightweight key generation-assisted homomorphic authenticated encryption.

References

1. <https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/ushering-in-a-better-connected-future>
2. Zhang Y, Xiang Y, Huang X, Chen X, Alelaiwi A (2018) A matrix-based cross-layer key establishment protocol for smart homes. *Inf Sci* 429:390–405

3. Mesmoudi S, Benadda B, Mesmoudi A (2019) SKWN: smart and dynamic key management scheme for wireless sensor networks. *Int J Commun Syst.* 32(7):e3930
4. Gebremichael T, Jennehag U, Gidlund M (2018) Lightweight IoT group key establishment scheme using one-way accumulator. *Computers and Communications (ISNCC), Rome, International Symposium on Networks*, pp 1–7
5. Goiuri Peralta, Cid-Fuentes Raul G, Josu Bilbao, Crespo Pedro M (2019) Homomorphic encryption and network coding in IoT architectures: advantages and future challenges. *Electronics* 8:827. <https://doi.org/10.3390/electronics8080827>
6. Chen YJ, Wang LC (2019) Privacy protection for Internet of Drones: a network coding approach. *IEEE Internet Things J* 6(2):1719–1730. <https://doi.org/10.1109/JIOT.2018.2875065>
7. Cheon JH, Han K, Hong SM, Kim HJ, Kim J, Kim S, Seo H, Shim H, Song Y (2018) Toward a secure drone system: flying with real-time homomorphic authenticated encryption. *IEEE Access* 6:24325–24339
8. Nafi M, Bouzefrane S, Omar M (2020) Matrix-based key management scheme for IoT networks. *Ad Hoc Netw* 97. <https://doi.org/10.1016/j.adhoc.2019.102003>
9. Singh A, Tentu AN, Venkaiah VC (2021) A dynamic key management paradigm for secure wireless ad hoc network communications. *Int J Inf Comput Secur* 14(3/4):380–402. <https://doi.org/10.1504/IJICS.2021.10029986>
10. Zhang Y, He D, Li L, Chen B (2020) A lightweight authentication and key agreement scheme for internet of drones. *Comput Commun.* <https://doi.org/10.1016/j.comcom.2020.02.067>
11. Vassilevska Williams V (2012) Multiplying matrices faster than Coppersmith-Winograd. *Proc ACM Symp Theor Comput (STOC)* 44:887–898
12. Lim LH (2013) Tensors and hypermatrices. In: Hogben L (ed) *Handbook of linear algebra*, 2nd edn. CRC Press, Boca Raton, FL
13. Blom R (1984) An optimal class of symmetric key generation systems. *Workshop on the theory and application of cryptographic techniques*. Springer, Heidelberg, pp 335–338
14. Zhang Y, Xiang Y, Huang X, Chen X, Alelaiwi A (2018) A matrix-based cross-layer key establishment protocol for smart homes. *Inf Sci* 429:390–405
15. Malina L, Srivastava G, Dzurenda P, Hajny J, Ricci S (2019) A privacy-enhancing framework for Internet of Things services. *eprint.iacr.org*. https://doi.org/10.1007/978-3-030-36938-5_5
16. Gheisari M, Wang G, ZadaKhan W, Christian F (2019) A context-aware privacy-preserving method for IoT-based smart city using software defined networking. *Comput Secur* 87:101470

Gas Leakage Detection and Control System



Sanjay Kumar, Durgesh Kumar, Deepanshu, and Abhishek

Abstract Gas leakage is one of the major and most common root causes of house fires that we regularly hear. These gasses do not even have any smell or color, making it even more difficult to detect any leakage by a person, and these incidents are increasing day by day. Nowadays, we hear very frequently about these cylinder explosions and fire incidents due to gas leakages which results in serious losses. It can detect, prevent, and alert the user too. Generally, the leakage detectors that are currently in the market can only detect leakage and alert via audio indication while we are also using the stepper motors too for turning off the valve and cutting the gas supply in case any leakage occurs and no one is present at home. We have also incorporated a feature that will increase the safety even further. We have added the feature to cut off electricity to the house as even a small leakage can turn into a deadly disaster from a little spark. The sensor which we have used can detect LPG, isobutane, propane, LNG, and smoke too.

Keywords IOT · Arduino · Relay module · Sensor · PPM · Cloud storage · Broadcast module · LCD display

1 Introduction

LPG is supposed to replace traditional cooking fuels in rural kitchens such as firewood and cow dung which not only contributes to environmental degradation but also has serious health implications on users. Still, there are many households in our country which are still using these traditional cooking fuels but now the rapid increase in population combined with LPG penetration in rural areas due to various governments programs and subsidies has resulted in an average growth of 8.4% in LPG consumption, making India the second largest consumer of LPG in the world at 22.5 million tones. LPG consumers have grown at a compounded annual growth rate (CAGR) of 15%—from 14.8 crore in 2014–15 to 22.4 crore in 2017–18.

S. Kumar (✉) · D. Kumar · Deepanshu · Abhishek
GB Pant Government Engineering College, New Delhi 110020, India
e-mail: sanjaykumar@gbpec.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023
S. C. Satapathy et al. (eds.), *Computer Communication, Networking and IoT*,
Lecture Notes in Networks and Systems 459,
https://doi.org/10.1007/978-981-19-1976-3_27

205

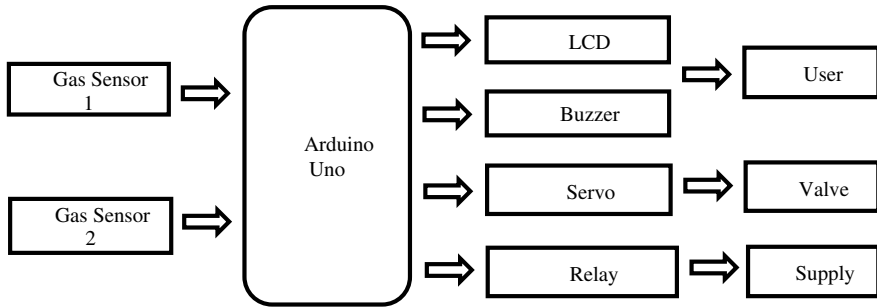


Fig. 1 Block diagram of gas leakage detection and control system

With this high growth rate of increase in consumers, the accidents are also bound to increase significantly. Many people have lost their lives and are still losing their own lives, their loved one's lives, and property by house fires caused by gas leakage. We are trying to prevent and minimize the loss by early detection of any leaks and informing everyone related to it as our cities are very densely populated with very small allies [1, 2]. So, the fire in one building can spread to others and can become a very huge disaster which will be very difficult to get under the control of firefighters as our streets and allies are very narrow for them. Also, the LPG penetration is occurring deep and deep in our remote villages, where it becomes even more difficult for our firefighters to cover up all the remote areas and be responsive on the time of accident as majority of the fire stations are situated in big cities. So, early leakage detection and prevention are the only option we have.

A few gas leakage monitoring and alerting systems based on IoT [3–5] have been suggested in the recent past so that the user gets significant alerts.

The block diagram of gas leakage detection and control system is shown in Fig. 1.

2 Literature Review

The authors [1] in their paper explained a new system that has been designed for gas alerts using Internet. This system can detect the level of gas and send an alert to the user. This system continuously senses its concentration in the air and displays it on the screen. Just when its concentration crosses the threshold, the buzzers start making noise and an alert message is sent to the user's email ID. The authors [2] in their research paper proposed a system for the detection of gas level which has two modules, one of which is gas detection module and other one is broadcasting module. This system was designed by her specifically for the domestic purpose and some specific industry applications too. In [6], a system is explained which was basically based on the integration of GSM with the gas detection system to make it automatic. This system was designed for leakage detection, alerting the user with a message, and on the top of that, it also stores the user data to further analyze the problem.

Subramanian and his team [7] in their research paper presented a technique by using an MQ5 gas sensor for leakage detection and Arduino Uno for data collection and its analysis. The amount of gas leaked is converted from PPM to volts by Arduino IDE, and the user is notified if it crosses the threshold value. Then, the user is alerted by an app and buzzer/LED for physical indication. The authors in [8] explained about introducing a mini mobile robot that is capable to detect the leakage in hazardous places. In the case of leakage, the robot will send the data immediately to android mobile linked to it via Bluetooth. Bluetooth is used in place of other methods like GSM and GPS because of their inefficiency for communication in particular areas, and an android application has also been developed for the robot which can receive the data directly from it. That app gets the notification of leakage and can also be used to control the robot's movement by text command or voice commands.

In 2016, the authors [9] proposed an embedded design integrated circuit and MQ9 sensor with switches, relays, solenoids, LEDs, LCD screens, and also some sensors for sensing temperature, humidity, light level, etc. for dangerous gas leakage detection and to remove human interaction completely from the process. The authors in [10] explained about their system in which they used a multipoint methane sensor which works using a DFB laser source with micro-optic cells and fiber-optic network. The sensitivity of their system was lowered down to very few PPM by using various methods for better leakage detection like digital signal processing and line scanning. But the system had some limitation in S/N ratio due to etalon fringes and also explained the way to minimize its effect. The authors in [11] presented their system which not only warns the user using on-site alarm but also sends the warning message to the first response team too in the case the user is not present at home. It uses FPGA to detect gas leakage and uses a GSM module for alert call. Then, a prototype was developed and designed upon LPG leakage. In [12], the authors presented gas leakage problem for the industrial sectors and vehicles that operate on gas like CNG, i.e., buses and cars. The method that they presented was to install a sensor that senses any leakage; then, the alert message is sent to the linked mobile number when the gas concentration crosses the threshold level; and then, the buzzers and LEDs are also turned on simultaneously for physical indication. In [13], the authors proposed a computer load distribution. Transmitted data's dynamic optimization is required for large scale monitoring. In this work, they used multiple wireless sensors making a network for the methane leakage detection. The chemiresistive sensors and wind sensors were used to aggregate all the data, and then, it was transmitted to the cloud for its analysis. This network of sensors was also integrated with the inversion model for location detection of the leak and to quantify the leakage rate. It is a robust system for long-term monitoring and for tracking the regulatory compliances.

3 Methodology

LPG gas leakage is detected by the MQ135/MQ6/MQ2 sensors, and MQ2 can detect many gases and smoke too, so we have used it in our system. The micro-controller

takes the output from the sensors and converts them from analog to digital signal using its inbuilt ADC. As the sensor detects any leakage, a signal is sent to the Arduino Uno for further processing where all the components are attached to each other. It has predefined sets which sends the signal to rotate the stepper motor as soon as the concentration of gas increases from the threshold value in the room, the rotating stepper motor further rotates the knob of the cylinder resulting in the stoppage of the gas supply, the buzzer also gets a signal simultaneously, and it gets activated too. This gives a physical indication to the user along with LCD screen and a LED bulb which warns the user with a warning message, a danger indicating red light and an alarming sound. One more layer of security [14] has been added to this system as the system detects the leakage and Arduino Uno sends one more signal to the relay module to cut off the electric supply of the house by tripping the MCB considering any fire incident may happen due to leaked gas and short circuit.

The simulation model of gas leakage detection and control system is shown in Fig. 2.

There are many similar papers that have already been developed on this topic but what makes our work unique is the automatic “Regulator Valve Control Arm” that we have developed in order to close the gas valve without interfering with the regulator design so that it automatically closes the valve as soon as it detects the leakage. We have used MG995 servo motor and have used clip on method to control the regulator effectively and securely that has been tested vigorously in real environment for proper functioning.

The regulator control arm is shown in Fig. 3.

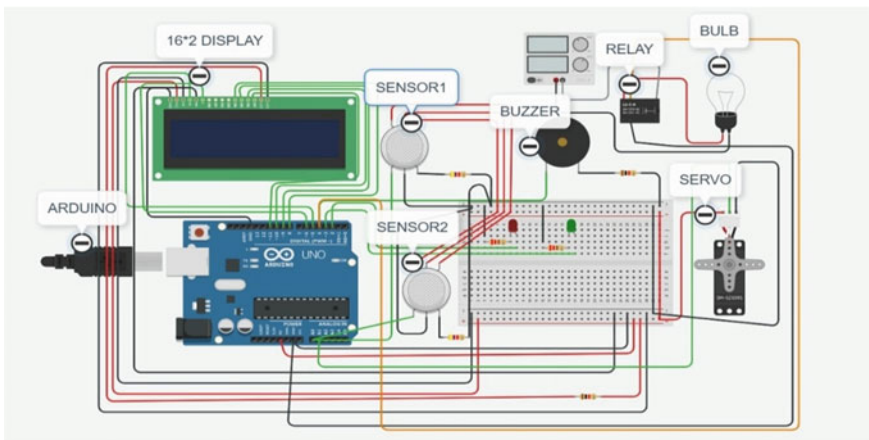


Fig. 2 Simulation model of gas leakage detection and control system

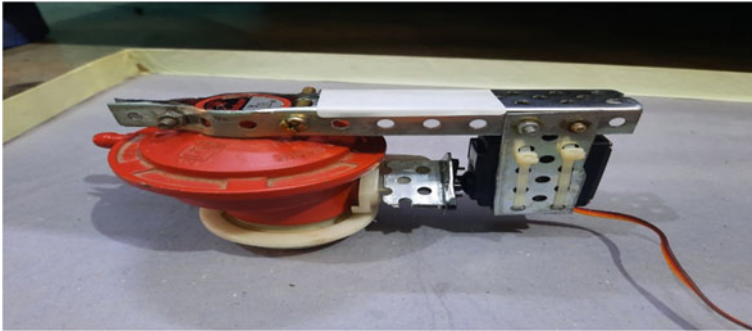


Fig. 3 Regulator control arm

4 Results

Firstly, the screen shows the message “Everything is OK” as the sensors have not detected any leakage yet and its concentration is below 35 (as shown in Fig. 4).

Now, the sensors have detected the leakage, and as its concentration increases and reaches above the set value of 35, the screen starts showing the warning message and alarm goes ON, and simultaneously, the gas valve is closed (as shown in Fig. 5).



Fig. 4 LCD screen before leakage detection



Fig. 5 LCD screen after leakage detection

Table 1 Threshold reading versus sensor reading

S. No.	Sensor reading	Threshold reading	Response
1	20	35	Everything ok
2	26	35	Everything ok
3	21	35	Everything ok
4	30	35	Everything ok
5	31	35	Everything ok
6	19	35	Everything ok
7	16	35	Everything ok
8	36	35	Leakage detected
9	39	35	Leakage detected

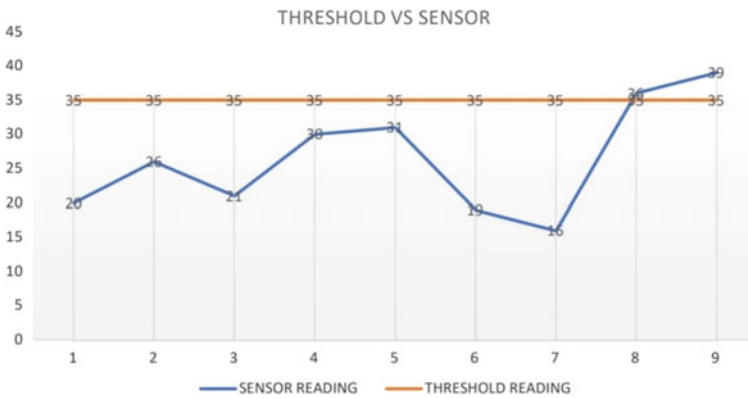


Fig. 6 Graphical representation of threshold versus sensor reading

Table 1 shows the tabular representation of threshold reading versus sensor reading.

Figure 6 is the graph between the threshold value and the sensor output value in which the sensor updates the value of gas concentration in atmosphere at every second. If anyhow the gas starts leaking, then the concentration of gas increases in atmosphere and it is updated by sensor.

5 Conclusion

Technological advancements have made it easier to carry out various daily tasks. Technology can be used in a variety of activities, including household cooking. But according to the studies, it is noted that the number of house fires caused by gas cylinders is still very high and a very little has been done regarding safety from its

leakage and fire prevention. Despite its grave consequences and importance, there has been close to none technological advancements in this regard. Exploding cooking gas cylinders and stoves accounted for nearly one-sixth of all deaths from accidental fires between 2010 and 2014, with a total of 19,491 deaths. So, this research work of ours is going to help a lot to the people and save a lot of lives and properties from the accidents due to any gas leakages, and if implemented properly, it can reduce these death rate statistics significantly.

References

1. Pandey RC, Verma M, Sahu LK, Deshmukh S (2017) Internet of things (IOT) based gas leakage monitoring and alerting system with MQ-2 sensor. *Int J Eng Dev Res* 5(2):2135–2137
2. Ramya P, Praveena V, Keerthiga S, Suresh A Smart gas level monitoring, leakage detection and registration over IOT
3. Sindhwani N, Maurya VP, Patel A, Yadav RK, Krishna S, Anand R (2022) Implementation of intelligent plantation system using virtual IoT. In: *Internet of Things and its applications*. Springer, Cham, pp 305–322
4. Anand R, Sindhwani N, Saini A (2021) Emerging technologies for COVID-19. In: *Enabling healthcare 4.0 for pandemics: a roadmap using AI, machine learning, IoT and cognitive technologies*, pp 163–188
5. Srivastava A, Gupta A, Anand R (2021) Optimized smart system for transportation using RFID technology. *Math Eng Sci Aerosp (MESA)* 12(4)
6. Imade S, Rajmanes P, Gavali A, Nayakwadi PVN (2018) Gas leakage detection and smart alerting system using IOT. *Int J Innovative Res Stud* 2(II)
7. Subramanian MA, Selvam N, Rajkumar S, Mahalakshmi R, Ramprabhakar J (2020) Gas leakage detection system using IoT with integrated notifications using Pushbullet—a review. In: *Fourth international conference on inventive systems and control (ICISC)*. IEEE, pp 359–362
8. Raju CM, Rani NS (2014) An android based automatic gas detection and indication robot. *Int J Comput Eng Appl* 8(1)
9. Falohun AS, Oke AO, Abolaji BM, Oladejo OE (2016) Dangerous gas detection using an integrated circuit and MQ-9. *Int J Comput Appl* 135(7)
10. Stewart G, Tandy C, Moodie D, Morante MA, Dong F (1998) Design of a fibre optic multi-point sensor for gas detection. *Sens Actuators, B Chem* 51(1–3):227–232
11. Arpitha T, Kiran D, Gupta VS, Duraiswamy P (2016) FPGA-GSM based gas leakage detection system. In: *IEEE annual India conference (INDICON)*. IEEE, pp 1–4
12. John AM, Purbia B, Sharma A, Udapurkar AS (2017) LPG/CNG gas leakage detection system with GSM module. *Int J Adv Res Comput Commun Eng* 6(5):536–540
13. Klein LJ, van Kessel T, Nair D, Muralidhar R, Hinds N, Hamann H, Sosa N (2017) Distributed wireless sensing for fugitive methane leak detection. In: *IEEE international conference on big data (big data)*. IEEE, pp 4583–4591
14. Anand R, Shrivastava G, Gupta S, Peng SL, Sindhwani N (2018) Audio watermarking with reduced number of random samples. In: *Handbook of research on network forensics and analysis techniques*. IGI Global, pp 372–394

Advanced Face Mask Detection System



Sanjay Kumar, Sandeep Kumar, Nirmalendu Kumar,
and Navneet Bhargava

Abstract COVID-19 pandemic caused a lot of loss and it is really important to give attention to technologies and ways to slow its spread and eventually stop it. Now in past few months, the government tried to open various sectors of society such as school gyms, etc. but failed and had to shut them down again due to increase in cases; we have seen a gradual increase in cases when the government tries to open these sectors because many persons were not so much attentive and were not following protocols properly. One of them is not wearing proper masks. Mask is a non-pharmaceutical measure that is used against primary spread of COVID by droplets. For people to follow protocols and wear masks, we are proposing a face mask detection device which will be effective to make people more aware to wear face masks by warning them who are not putting masks on their faces and restricting them to enter public places such as school, colleges, gym, etc.

Keywords Face detection model · Mask detection model · Data collection · Detection

1 Introduction

The pandemic of COVID-19 has been very much existent during the month, according to the latest WHO report, with approximately 44 lakhs more cases reported between August 30, 2021, and September 21, 2021. Globally, almost 220 million cases have been reported, with 4.5 million deaths [1]. According to the latest data from who SEAR, there are 42,203,618 confirmed cases and 663,310 deaths [1] There are 33,289,579 total cases in India, with 443,213 deaths, and the number of cases continues to rise [2].

This gives more of reason to focus on technology to make this fight against corona more effective which takes us to our project advanced COVID mask detection system. This framework identifies people without a mask and will give warning to them and

S. Kumar · S. Kumar · N. Kumar · N. Bhargava (✉)
GB Pant Government Engineering College, Okhla Phase-3, New Delhi 110020, India
e-mail: navneetbhargava789@gmail.com

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023
S. C. Satapathy et al. (eds.), *Computer Communication, Networking and IoT*,
Lecture Notes in Networks and Systems 459,
https://doi.org/10.1007/978-981-19-1976-3_28

213

hence restricting them from entering public places or schools and colleges etc. This project is based on measures to take against people not following protocol and are putting themselves in danger.

We are using system based on machine learning (ML) [3, 4] for training a model by edge impulse using raspberry pi and model will scan face using raspberry pi camera which will detect if the person in front of camera is wearing a mask or not, and if not, it will generate an alert and give warning and would not allow the person to enter the premises. It will make a person wear a proper mask to allow that person to pass. This is the primary stage and purpose of our project. As its primary stage finishes in the secondary stage, we will gradually make it complex as our project emerges and will introduce some more attributes to it. Further development can be done after primary stage, and we can make this device to be able to automatically shut gates and to scan body temperature at the same time with some further more research [5, 6].

1.1 OpenCV

It is a library which is mainly used for video capturing image processing and analysis [7]. It has features like face and object detection and uses color conversion and resizing of data images.

1.2 TensorFlow

TensorFlow is a source software library (based on open source) from Google for the analytical operation using the graphs based on the flow of data. TensorFlow bundles so many deep learning (DL)-based and ML-based algorithms and models. It allows us to use Python language in ML and provides a pre-API to build applications. C++ is used with TensorFlow and gives high performance running those applications.

1.3 Keras

Keras is an open-source library of state-of-the-art neural network, written via Python able to work adequately on TensorFlow. It is created by one of Google's engineers, Francois Chollet. It is designed to be user-friendly, flexible, and a module to aid rapid exploration through deep neural networks. It not only supports convolution networks and duplicate networks individually but also their combinations.

1.4 Imutils

Imutils is a series of simple tasks for doing the simple digital image processing operations such as translating, rotating, sketching, and displaying Matplotlib library images easily with OpenCV.

1.5 MobileNetV2

The MobileNetV2 architecture (shown in Fig. 1) is based on a degraded residual structure where the input and output of the existing block are small bottle layers that are contrary to the existing models using the MobileNetV2 input extensions using shallow flexibility to filter features are in the middle expansion layer. Additionally, we find that it is important to remove nonlinear lines from the thin layers in order to maintain the strength of the representation. We show that this improves performance and provides intuition that led to this design. The tutorial method allows the input of input/output domains in the expressiveness of transformation, which provides a simple framework for further analysis. We measure our performance in the ImageNet category, the acquisition of a COCO object, VOC image separation [8].

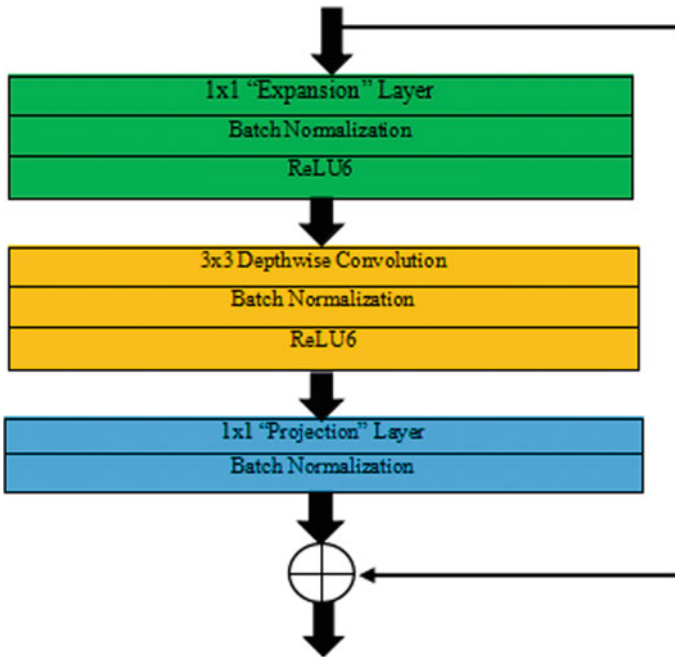


Fig. 1 MobileNetV2 architecture structure

1.6 Related Work

In [5], the authors presented how we can construct the classifier by using deep learning techniques that will collect the image of a person wearing a mask or without mask with better accuracy. We can also see the image with or without a mask in real-time video. In [5] Rosebrock, author tells us how to create a COVID-19 facial mask scanner using OpenCV, Keras/TensorFlow, and deep learning. To build face detector, the authors have trained a model with two categories of masked people and maskless people. They optimized MobileNetV2 for our mask/non-masking site and found the category with almost 99% accuracy. In [9], the authors developed a computerized scanning system to automatically detect violations of human masks in order to ensure their safety in infrastructure projects during the epidemic. To get a face mask, a set of data collected and described 1000 images, including various types of face masks, and added to the existing face mask website to create 1853 photo website. A number of high-resolution TensorFlow detection models were then developed on the face mask website, and the fastest mobile network MobileNetV2 was selected with 99.8% accuracy. The rotation matrix is used to remove the effect of the camera angle on the object in the image. This paper also used training for transfer learning model. In Sandler et al. [10], we learn about the depth of the MobileNetV2 architecture, which helps to improve the accuracy and efficiency of trained models. The strategy also improved the computer's efficiency.

2 Methodology

2.1 Data Set Collection

We took 12 k datasets of images from Kaggle mask that are pre-defined. The total images consist of 5000 with mask and 5000 without mask, and after that, it splits into training and testing data analysis of images.

2.2 Model Training

A default OpenCV module is used for obtaining the images followed by training a Keras model to identify the face mask.

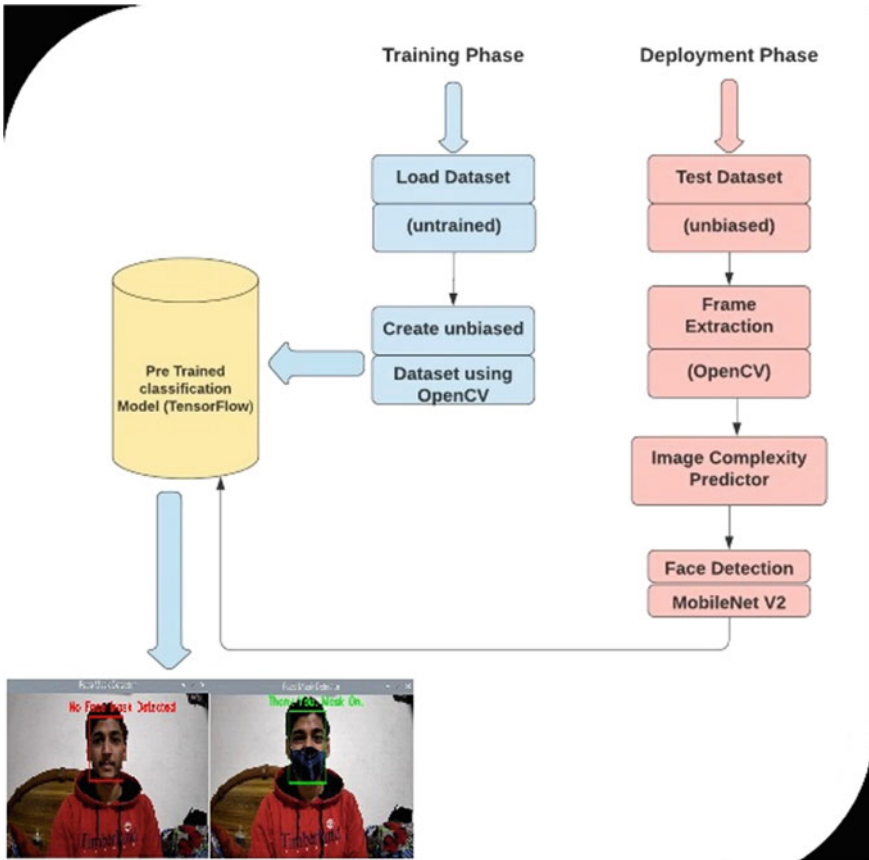


Fig. 2 Image processing block diagram

2.3 Detection

An OpenCV module is used to scan the face of people having a mask [11–13] by referring to the dataset which we took from Kaggle Face Mask 12 K Images Dataset. After detection if the person wear mask, then it will show the result by labeling it mask, and in case of face mask not being detected, it will show the result no mask.

The block diagram for image processing is shown in Fig. 2.

3 Results

Our device’s outcome is carried out by a laptop, in which we successfully identified a person using a mask and a person with no mask and operated appropriately.

Using Python, OpenCV, TensorFlow, and MobileNetV2, we successfully trained our model. We categorized our system into two classes, one without a mask and the other with a mask, so that it can find out whether a person is using a face mask or not, and we used the MobileNetV2 architecture to provide improved accuracy and computation methods (Fig. 3).

The graph shown in Fig. 4 shows training loss, validation loss, training accuracy, and validation accuracy with respect to number of epochs. Here, validation accuracy is more than training accuracy which shows that we do not have to insert more data (as it is accurate), and no more training is required. When it comes to training loss, it reaches close to the validation loss and gets low that shows that our model is working well and our model is right for this data.



Fig. 3 Live mask detection

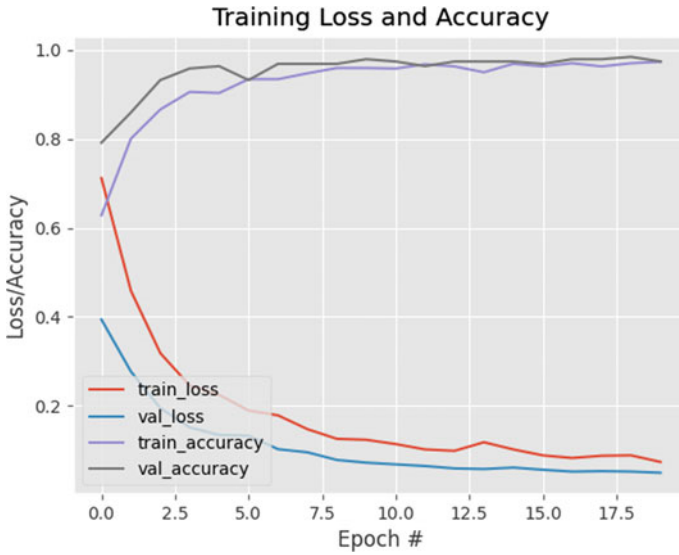


Fig. 4 Training loss and accuracy graph

4 Conclusion

With the rising number of COVID instances around the world, a technology that can check masks on people’s faces without the need of humans is desperately needed. Governments in several countries require masks to be worn in public places and congested regions. It is quite difficult to keep track of crowds at these locations. It is critical to detect persons not putting masks on their faces in order to stop the spreading of this pandemic. We summarized the techniques for identifying the masks using basic ML tools and simplified procedures in this research work and indicate how the method has attained a reasonable level of accuracy. Images and real-time video feeds with various occlusions and facial angles were used to test the suggested method. We suggest that this technique may effectively limit the exposure distance and perform effective control due to COVID-19’s worldwide influence. In addition, the research suggests a beneficial method for combating the problem.

References

1. www.who.int/southeastasia
2. <https://www.worldometers.info/coronavirus/>
3. Kamalraj R, Neelakandan S, Kumar MR, Rao VCS, Anand R, Singh H (2021) Interpretable filter based convolutional neural network (IF-CNN) for glucose prediction and classification using PD-SS algorithm. Measurement 183:109804

4. Singh H, Rehman TB, Gangadhar C, Anand R, Sindhwani N, Babu M (2021) Accuracy detection of coronary artery disease using machine learning algorithms. *Appl Nanosci* 1–7
5. Rosebrock A (2020) Covid-19: face mask detector with opencv, keras/tensorflow, and deep learning. [https://www.pyimagesearch.com/2020/05/04/covid-19-face-mask-detector-wit hopencv-keras-tensorflow-and-deeplearning](https://www.pyimagesearch.com/2020/05/04/covid-19-face-mask-detector-with-opencv-keras-tensorflow-and-deeplearning)
6. Sung KK, Poggio T (1998) Example-based learning for view-based human face detection. *IEEE Trans Pattern Anal Mach Intell* 20(1):39–51
7. Saini P, Anand MR (2014) Identification of defects in plastic gears using image processing and computer vision: a review. *Int J Eng Res* 3(2):94–99
8. Goyal B, Dogra A, Khoond R, Gupta A, Anand R (2021) Infrared and visible image fusion for concealed weapon detection using transform and spatial domain filters. In: 9th international conference on reliability, Infocom technologies and optimization (trends and future directions)(ICRITO). IEEE, pp 1–4
9. Suganthalakshmi R, Hafeeza A, Abinaya P, Ganga Devi A (2021) Covid-19 facemask detection with deep learning and computer vision. *Int J Eng Res Tech (IJERT) ICRADL*
10. Sandler M, Howard A, Zhu M, Zhmoginov A, Chen LC (2018) Mobilenetv2: inverted residuals and linear bottlenecks. In: *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp 4510–4520
11. Razavi M, Alikhani H, Janfaza V, Sadeghi B, Alikhani E (2022) An automatic system to monitor the physical distance and face mask wearing of construction workers in COVID-19 pandemic. *SN Comput Sci* 3(1):1–8
12. Eikenberry SE, Mancuso M, Iboi E, Phan T, Eikenberry K, Kuang Y, ... Gumel AB (2020) To mask or not to mask: modeling the potential for face mask use by the general public to curtail the COVID-19 pandemic. *Infect Dis Model* 5:293–308
13. Sethi S, Kathuria M, Kaushik T (2021) Face mask detection using deep learning: an approach to reduce risk of coronavirus spread. *J Biomed Inform* 120:103848

Meta-Analysis of Nanostructured Sensors for Toxic Gas Sensing



Saumya Srivastava, Tripti Sharma, and Manish Deshwal

Abstract This paper exploring the metal oxide semiconductor (MOS) gas sensors with major focus to enhance the performance of the gas sensor by exploring the different parameters. Literature analysis is carried out here for better understanding the do-pants effect. The advancements in technology opted for the manufacturing of the sensor includes the development in miniaturization technology, speed enhancement and lowering down the cost. As per the need says development of sensor should be done in such a manner that it reflects efficiency, reliability and good quality in the domestic and commercial field. The main application of gas sensor is to sense the toxic gas such as acetone, toluene, CO, NO₂ and SO₂ from the environment. This paper will help to find out different methodology to detect the harmful gases as well as which material is suitable to detect the particular gas. Today, many researchers focus towards in the area of sensors because these sensors make human live easy. In this paper, a detailed survey has been covered mainly for gas sensor primarily based on different material, for various temperature as well as different in addition to recognize special gases.

Keywords Gas sensor · Selectivity · Operating temperature · Accuracy · Sensitivity · Resolution

S. Srivastava (✉) · T. Sharma · M. Deshwal
Department of Electronics and Communication Engineering, Chandigarh University, Gharuan,
Punjab, India
e-mail: saumya.e8420@cumail.in

T. Sharma
e-mail: triptisharma.ece@cumail.in

M. Deshwal
e-mail: deshwal.manish@gmail.com

1 Introduction

In this modern era, to make human live easy and healthy, different sensors are used here for sensing various physical quantities. Sensors arrangement are based on applied stimuli which are thermal, acoustic, electric, optical, and magnetic and so forth [1–3]. Semiconducting metal oxide-based sensors are now major significant interest towards the researcher of nano-innovation. In the gas sensor, one topology is used here, i.e., “chemo-resistivity.” Chemo-resistive gas sensor is based on the phenomena to change resistance of semiconducting sensing element in presence of oxidizing and reducing gas. The major parameters to check the sensors credibility is primarily based upon sensitivity. Sensitivity is a parameter by means of the help of this sensor performance can be checked [4, 5]. So can be say that, to enhance the quality of the sensor, sensitivity of the device should be increased as well as good selectivity and stability is required. Sensors can be based on temperature, pressure, liquid, gas, etc. For more application in present situation, gas sensors are very useful [6, 7]. Gas sensor is used in the time of leakage of LPG gas, nitrogen gas, carbon dioxide gas, etc.

Sensors are used for meals testing, medical care tool, water testing and biological war agent detection. Bio-sensors are very beneficial in modern technology. These are based at the CMOS era. They are utilized in patron electronics, biometric, visitors and safety surveillance and PC imaging. Image sensors are very beneficial in scientific and non-medical subject. These are based totally on the infrared, ultrasonic and microwave/radar generation [6–10]. Now, one of the miniaturization devices through nano-technology is named as transducer which transforms one form of energy to other form finds its suitable applicability [11]. One can find the applications of transducers for utilization in any device that is to be miniaturized and fabrication onto a single chip. Transducers are mainly used for the detection of physical signals for processing and then providing signals to actuate the related process [12–14]. These are diverse sensors to be had within the marketplace based totally on acceleration. The micro-electro mechanical sensors are useful in one of a kind technology are very useful within the different industries. They are used for patient tracking which includes pace makers and car dynamic structures [15–18].

Sensors are used for food testing, medical care device, water testing and biological wafer agent detection. Bio-sensors are very useful in modern era. These are based on the CMOS technology [15]. They are used in consumer electronics, biometric, traffic and security surveillance and PC imaging. Image sensors are very useful in medical and non-medical field. These are based on the infrared, ultrasonic and microwave/radar technology [16–18]. They are used in videogames and simulations, light activation and security detection.

2 Gas Sensing Platforms

In this section, various approaches and techniques have been introduced here for detection of gases/vapors. There are multiple techniques available for detecting gas sensitivity but out of all, semiconductor sensor is mostly used for detecting target gases.

- (i) Semiconductor sensor:
- (ii) Chromatography
- (iii) IR spectroscopy
- (iv) Electrochemical sensor
- (v) Surface acoustic wave-based sensor
- (vi) Surface Plasmon resonance sensor.

(i) **Semiconductor Sensor:**

This technique is basically works on chemo-resistive principle where by changing the resistivity or conductivity of semiconductor sensing material by interaction with the target gas can be recorded and help to measure the sensitivity of the particular gas towards the particular material.

(ii) **Chromatography**

This technique is based on the separation and analysis of the mixture of compound. Most widely used applications of this technique is identification and analysis of different drugs.

(iii) **IR spectroscopy**

IR spectroscopy technique and sources basically induce some molecular vibrations for the excitation of higher levels within range for wave numbers of $4000\text{--}200\text{ cm}^{-1}$ and rise the absorption band due to chemical bonds and samples.

(iv) **Electrochemical Sensor**

Electrochemical sensor is worked on the principle of change electrochemical properties for working of electrode during the interaction with gas molecular. In this technique, three electrodes are used, i.e., reference electrode, measuring electrode as well as counter electrode. These sensors are used for determining the partial pressure of oxygen molecules in the ambient air or the concentration of toxic gases.

(v) **Surface Acoustic wave based Sensor**

Surface acoustic wave (SAW) sensors are based over the principle of mechanical vibrations propagating over the surface of a piezoelectric material deposited over a lower density medium. The working of a SAW-based sensor can be explained using the principle of changing propagation characteristics of SAW waves like velocity, in-order phase and attenuation of the signal on interacting with target gas molecules.

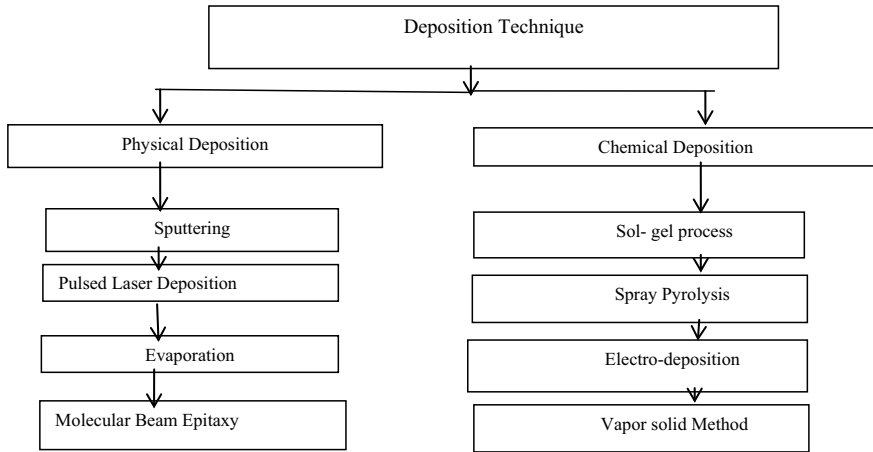


Fig. 1 Different deposition techniques

(vi) **Surface Plasmon resonance Sensor**

SPR technique is very sensitive technique for gas and chemical sensing. Surface Plasmons (SPs) are the collective charge density oscillations that may possibly exist at the interface of two dielectric media with opposite charges.

Figure 1 indicates the different deposition techniques of thin film in gas sensor. These techniques are classified as chemical and physical deposition. This technique is further classified as sputtering, pulsed laser deposition, evaporation and molecular beam epitaxy as well as sol gel, spray pyrolysis, electro-deposition and vapor–solid method. Out of all, these technique sol–gel method is used for synthesis the ZnO. Table 1 represents a detail review included for gas sensor. In this table, we discussed about different material used for thin film formation and included different doped atoms which are helpful for enhancing the sensitivity of the gas sensors as well as selectivity. One important parameter of gas sensor is operating temperature, so this table will help to find out which temperature are more useful for different operating temperature, and how their sensitivity change accordingly [8–11].

Table 1 represents the tabular way to provide a complete comparison between different material, different do-pants a as well as different operating temperature, how sensitivity of the gas sensor is enhance towards the particular gas. In Table 1, different columns are introduced, i.e., based on different materials, different methodology, different gases as well as sensing of gases at different ppm level. During survey, it is analyzed that, dynamic range of the particular gas should be wide for effective sensing.

Here, tabular represents clearly shows that most of the research is carried out on ZnO or SnO₂ as a sensing material towards different gases H₂, CO, NO, NO₂, etc., and many more research has to be used to be go through in different toxic gases especially in NO_x, and Fig. 2 indicates that during the survey, it is identified that SnO₂ and ZnO are broadly used for sensing different gases. There are also lots of works

Table 1 Tabular representation of different gas sensors based on different materials

Ref. No.	Year	Material used	Doped atoms	Operating temp (°C)	Sensitivity (response)	Method	Gas conc. (ppm)	Target gas
[5]	2005	Ē-Al ₂ O ₃	Ē-Al ₂ O ₃	450	–	XRD, SEM	3500	CO, CO ₂
[6]	2005	SmFeO ₃	SmFeO ₃	290, 390	10	XRD, XPS, FESEM	0.01	NO ₂
[7]	2005	T-ZnO and G-ZnO		320, 420	90%	SEM observation	100	
[8]	2006	MnO ₂ and TiO ₂		197		DBD plasma detector	300–380	CO, CO ₂
[9]	2006	Co/ZrO ₂	Co ₃ O ₄	180		XRD, TRP	300	
[10]	2006	FeCl ₃	Polypyrrole	25, 70		SEM	300–1000	
[11]	2007	Ce-Ti-O	Au	400	63%	Sol-gel method		
[12]	2007	CsX, NaX	Isopropanol	250	80%			CO ₂
[13]	2007	Zeolite FAU, ZrO ₂	Pd or Cu	600				CO ₂
[14]	2008	WO ₃		350, 450		RF sputtering		NO
[15]	2008	CeO ₂ , SnO ₂ , ZrO ₂ , Al ₂ O ₃	Ru	800		XRD		H ₂ , N ₂
[16]	2008	Al pillared bentonite	Cr and Pd	600	90%	XRD and TG		HCL, Cl ₂
[17]	2008	Ce-Ti-O	Au	600		XRD	6000	H ₂
[18]	2009	Manganese oxide	Carbon/Carbon xerogel	240	100	TPD, TG-DSC		Ethanol
[19]	2009	MCM-41	Toluene	260–596	50	XRD, TEM, TPR		
[20]	2010	ZnO		400	100	RF sputtering	500	
[21]	2010	CeO ₂	Au	300, 500	100			

(continued)

Table 1 (continued)

Ref. No.	Year	Material used	Doped atoms	Operating temp (°C)	Sensitivity (response)	Method	Gas conc. (ppm)	Target gas
[22]	2010	Pt/CeO ₂ -ZrO ₂ -Bi ₂ O ₃ /Ē-Al ₂ O ₃	Pt/CZB/Al ₂	120		FID, TCD	900	N ₂
[23]	2010	WO ₃ -SnO ₂		100-300, 800		BET, XRD, TEM, TPD, XPS	186-200	NO ₂
[24]	2011	Cu-Mn and Co-Mn	Cu-Mn and Co-Mn	300, 468	90	XRF, XRD, TPR	1200	
[25]	2011	TiO ₂	HF	200		XRD, SEM, EDX	5000	CCl ₄
[26]	2012	Manganese and cerium oxides	Pure oxides and Au	230, 250, 300	100	FESEM-EDS, XRD, XPS, HRTEM, HAADF and ICP-AES		Ethyl acetate, ethanol and toluene
[27]	2012	Porous NiO	Au electrode and platinum wires	400		XRD, SEM, TEM	5-1000	Ethanol, acetone, methanol and formaldehyde
[28]	2012	TiO ₂	Dry nitrogen atmosphere	450, 600			400-1600	Ethylene
[29]	2013	2013	H ₂ O ₂	450		XRD, SEM, TEM, EDS, FSEM		N ₂
[30]	2013	HZSM-5	CeO ₂ , Cr ₂ O ₃	350	79 and 77	DCE, DCM, TCE		Cl ₂
[31]	2013	CeO ₂ -Al ₂ O ₃	Pt	250	100	Sol-gel method		CO ₂

(continued)

Table 1 (continued)

Ref. No.	Year	Material used	Doped atoms	Operating temp (°C)	Sensitivity (response)	Method	Gas conc. (ppm)	Target gas
[32]	2013	Ce _{1-x} Sm _x O ₈	Cu	260		XRD, XPS, TPR, SEM		CO ₂
[33]	2014	CNT	Pt	40–150		SEM, TEM, XRD, XPS, EDS	100–500	CO ₂
[34]	2014	CuO and NiO	Au	– 196		SEM, DIM, EDS, XPS		N ₂
[35]	2014	In ₂ O ₃	Au	200–350	99.99	XRD, SEM, XPS, EDS	100–2000	
[36]	2014	SmFeO ₃	Pt/AI	350–500	90		10	
[37]	2015	CuO	Cu	200	99.99	XRD, SEM,	20–500	CCl ₄
[38]	2015	Mn ₂ O ₄ , Mn ₃ O ₄ , Mn _x O _y		310	92	XPS, XRD, TEM, TPR		CO ₂
[39]	2015		Co–Mn	<400	90	XRF, XRD, TPR, SEM		CO ₂
[40]	2015	CeO ₂	Pt	160–180	80	XPS, TPR		CO ₂
[41]	2016	BiWO ₆ /CQD		150, 60		TEM, DRS, XPS, XRD, SEM		CO ₂
[42]	2016	SnO ₂	Pd, Pt and Au	250	90	TPR, TEM		NO
[43]	2016	ZnO	UV	220		XRD, SEM, TEM	10–1000	

(continued)

Table 1 (continued)

Ref. No.	Year	Material used	Doped atoms	Operating temp (°C)	Sensitivity (response)	Method	Gas conc. (ppm)	Target gas
[44]	2017	SnO ₂	Ag	160, 200		XRD, XPS, TEM, SEM, BET	5–50 ppm	Acetone
[45]	2017	YSZ, solid electrolyte	Au	400–500		SEM	0.5–50	Toluene
[46]	2018	NiO/ZnO	Au			SEM, TEM	7–11 ppm	Ethanol, acetone
[47]	2018	Co ₃ O ₄ slices/reduced graphene oxide hybrid		200, 500		TEM, FESEM, XRD, EDS	5	NO ₂
[48]	2018	WO ₃	Si	75–300, 500		SEM, XRD, Raman, XPS	10	NO ₂
[49]	2019	WO ₃	Pt	180–280, 440		SEM, XRD, Raman, XPS	50	
[50]	2019	SnO ₂ , SnS ₂	Au	>350, 200		EDX, XPS, HRTEM, XRD, XPS		Acetone
[51]	2019	Fe ₂ O ₃ , MoO ₃		223		XRD, SEM, TEM, EDX, EDS, XPS	100	Xylene
[52]	2019	In ₂ O ₃		300		XRD, TEM, XPS	1–100	CH ₃ CHO
[53]	2020	Co ₃ O ₄	2-Propanol	160		SEM, FESEM, BET, XRD, HETEM, XPS		

(continued)

Table 1 (continued)

Ref. No.	Year	Material used	Doped atoms	Operating temp (°C)	Sensitivity (response)	Method	Gas conc. (ppm)	Target gas
[54]	2020	Cerium-copper-manganese oxide	Solution combustion synthesis	250		XRD, FESEM, TPR, XPS		CO, CO ₂
[55]	2020	Tungsten oxide		60–270		XRD, SEM, Sol gel method		
[56]	2021	Pt/SnO ₂			1758s 4071s	Sol-gel method		CO, NO _x , C ₃ H ₈
[57]	2021	WO ₃ , WS ₂ and MoS ₂		27		Vacuum filtration technique	0.7–3.5 ppm	NO _x

Materials Utilization

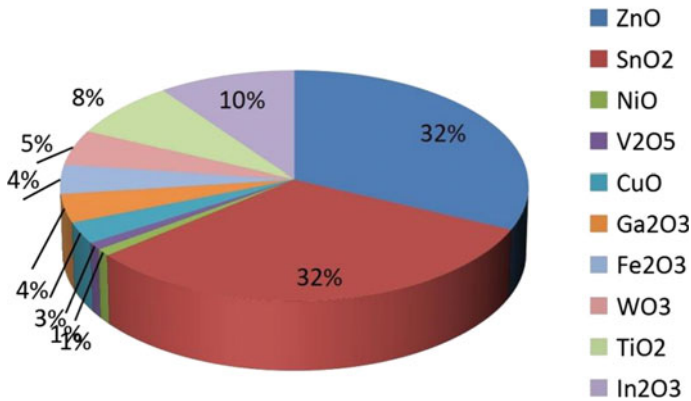


Fig. 2 % material utilization for gas sensor

which are going on NiO, V₂O₅, CuO, Ga₂O₃, Fe₂O₃, WO₃, TiO₂ and In₂O₃ material for different gas sensing. According to literature survey, it is observed that there are different types of gas sensors available for different applications. These sensors are solid electrolyte, infrared absorption, electro chemical, thermal conductivity as well as metal oxide semiconductor sensor. Based on the sensing methods, gas sensors are classified as by changing electrical property as well as other properties [56].

(a) Performance of gas sensors

Gas sensor performance can be evaluated using selectivity, sensitivity, stability, response time as well as recovery time. Sensitivity can be defined in different form for reducing gas as well as oxidizing gases. Sensitivity can be expressed as R_a/R_g for reducing gases and R_g/R_a for oxidizing gases, where R_a : resistance in air, R_g : resistance for reducing gas or oxidizing gas. Percentage sensitivity is expressed by $[(R_a - R_g)/R_a] * 100\%$ [57].

Second important parameter is selectivity, i.e., defined as to find out the specific gas (target gas) out of other gas. Next important parameter is response time and recovery time [52–54].

(b) Major Properties of Metal oxide Semiconductor used for gas sensing

There are several methods available for optimizing the parameter [58, 59]. By changing the grain size of micro-structure device, the sensitivity of the device will be increase [60, 61]. When the grain size (D) $\gg 2L$ (thickness of the space charge layer), the conductance is limited by Schottky barrier at grain boundaries (known as grain boundary control). If $D = 2L$, conductance is limited by necks between grains (known as neck control), and if $D < 2L$, conductance is influenced by every grains (known as grain control) During literature survey, it is noticed that sensitivity of the gas sensor depends on film thickness and this film thickness can be controlled by controlling the sputtering

time, and sputtering deposition is carried out at ambient temperature and film thickness will vary by adjusting the sputtering duration. Another method for improving gas sensitivity is changing porosity [22–27].

(c) **Factors affecting the selectivity and sensitivity of semiconductor metal oxide gas sensors**

There are two major things achieve to enhance the selectivity of the semiconductor metal oxide gas sensor in this first method is to synthesize a material which is selective in particular compound, and second one is to discriminate between mixture [28–31]. By adding do-pants selectivity of the gas sensor will improve.

3 Conclusion

In this paper, it is clearly mentioned that sensors are very essential term in this modern era, especially gas sensor has important role to detect toxic gases from the environment. In this paper, a tabular review is introduced in which it is clearly mentioned how different thin film-based gas sensor reacts on different temperature for particular gas. Sensitivity and concentration of particular gases are also mentioned. Whenever operating temperature is increased, sensitivities of the gas sensor is increased. The sensitivity of the gas sensor can be improved by using doping noble metal or metal oxides inside the thin film. In gas sensor, important parameters are sensitivity, selectivity and response and recovery time. After literature, it can be concluded that most of the gas sensors are fabricated on ZnO and SnO₂-based thin film for different gases and response and recovery time should be fast for more improvement in the gas sensor. For effective response, dynamic range of the device should be high so that it can detect low ppm gas as well as high ppm. This paper will help to researcher to find out that particular material as well as operating temperature is good for particular target gas.

References

1. Travis CC, Hester ST (1991) Global chemical pollution. *Environ Sci Technol* 25:814–819
2. Gorell JM, Johnson C, Rybicki B, Peterson E, Richardson R (1998) The risk of Parkinson's disease with exposure to pesticides, farming, well water, and rural living. *Neurology* 50:1346–1350
3. Johns T, Sthapit BR (2004) Biocultural diversity in the sustainability of developing-country food systems. *Food Nutr Bull* 25:143–155
4. Sharma S, Kumar S, Singh B (2015) Routing in wireless mesh networks: three new nature inspired approaches. *Wirel Pers Commun* 83:3157–3179
5. Roland U et al (2005) Combination of non-thermal plasma and heterogeneous catalysis for oxidation of volatile organic compounds: part 2. Ozone decomposition and deactivation of γ -Al₂O₃. *Appl Catal B: Environ* 58(3–4):217–226
6. Hosoya Y et al (2005) Ozone detection in air using SmFeO₃ gas sensor. *Sens Actuators B: Chem* 108(1–2):198–201

7. Zhu BL et al (2005) The gas-sensing properties of thick film based on tetrapod-shaped ZnO nanopowders. *Mater Lett* 59(8–9):1004–1007
8. Lu B, Zhang X (2006) Catalytic oxidation of benzene using DBD corona discharges. *J Hazard Mater* 137(1):633–637
9. Wyrwalski F et al (2006) Influence of the ethylenediamine addition on the activity, dispersion and reducibility of cobalt oxide catalysts supported over ZrO₂ for complete VOC oxidation. *Catal Lett* 87–95
10. Lim C-B et al (2006) Sensing characteristics of nano-network structure of polypyrrole for volatile organic compounds (VOCs) gases. *IEEE*
11. Gennequin C et al (2007) Catalytic oxidation of VOCs on Au/Ce–Ti–O. *Catal Today* 122(3–4):301–306
12. Beauchet R (2007) Catalytic oxidation of volatile organic compounds (VOCs) mixture (isopropanol/o-xylene) on zeolite catalysts. *Catal Today* 124(3–4):118–123
13. Tidahy HL (2007) Catalytic activity of copper and palladium based catalysts for toluene total oxidation. *Catal Today* 119(1–4):317–320
14. Vallejos S et al (2008) Micro-machined WO₃-based sensors selective to oxidizing gases. *Sens Actuators B: Chem* 132(1):209–215
15. Mitsui T et al (2008) Support effect on complete oxidation of volatile organic compounds over Ru catalysts. *Appl Catal B: Environ* 81(1–2):56–63
16. Oliveira LCA et al (2008) Catalytic oxidation of aromatic VOCs with Cr or Pd-impregnated Al-pillared bentonite: by product formation and deactivation studies. *Appl Clay Sci* 39(3–4):218–222
17. Lamallem M et al (2008) Effect of the preparation method on Au/Ce–Ti–O catalysts activity for VOCs oxidation. *Catal Today* 137(2–4):367–372
18. Bastos SST et al (2009) Manganese oxide catalysts synthesized by exotemplating for the total oxidation of ethanol. *Appl Catal B: Environ* 93(1–2):30–37
19. Popova M et al (2009) Toluene oxidation on titanium- and iron-modified MCM-41 materials. *J Hazard Mater* 168(1):226–232
20. Al-Hardan NH et al (2010) ZnO thin films for VOC sensing applications. *Vacuum* 85(1):101–106
21. Delannoy L et al (2010) Supported gold catalysts for the decomposition of VOC: total oxidation of propene in low concentration as model reaction. *Appl Catal B: Environ* 94(1–2):117–124
22. Masui T et al (2010) Total oxidation of toluene on Pt/CeO₂–ZrO₂–Bi₂O₃/γ-Al₂O₃ catalysts prepared in the presence of polyvinyl pyrrolidone. *J Hazard Mater* 176(1–3):1106–1109
23. Bai S et al (2010) Preparation, characterization of WO₃–SnO₂ nanocomposites and their sensing properties for NO₂. *Sens Actuators B: Chem* 150(2):749–755
24. Aguilera DA et al (2011) Cu–Mn and Co–Mn catalysts synthesized from hydrotalcites and their use in the oxidation of VOCs. *Appl Catal B: Environ* 104(1–2):144–150
25. Kılınc N et al (2011) Fabrication of TiO₂ nanotubes by anodization of Ti thin films for VOC sensing. *Thin Solid Films* 520(3):953–958
26. Bastos SST et al (2012) Total oxidation of ethyl acetate, ethanol and toluene catalyzed by exotemplated manganese and cerium oxides loaded with gold. *Catal Today* 180(1):148–154
27. Dong C et al (2015) Porous NiO nanosheets self-grown on alumina tube using a novel flash synthesis and their gas sensing properties. *RCS Adv* 5:4880–4885
28. Geng Q et al (2012) The correlation between the ethylene response and its oxidation over TiO₂ under UV irradiation. *Sens Actuators, B Chem* 174:449–457
29. Ma X et al (2013) Interfacial oxidation–dehydration induced formation of porous SnO₂ hollow nanospheres and their gas sensing properties. *Sens Actuators, B Chem* 177:196–204
30. Yang P et al (2013) Enhanced catalytic activity and stability of Ce doping on Cr supported HZSM-5 catalysts for deep oxidation of chlorinated volatile organic compounds. *Chem Eng J* 234:203–210
31. Sedjame H-J et al (2014) On the promoting effect of the addition of ceria to platinum based alumina catalysts for VOCs oxidation. *Appl Catal B* 144:233–242

32. Konsolakis M et al (2013) Redox properties and VOC oxidation activity of Cu catalysts supported on Ce_{1-x}Sm_xO₈ mixed oxides. *J Hazard Mater* 261:512–521
33. Joung H-J et al (2014) Catalytic oxidation of VOCs over CNT-supported platinum nanoparticles. *Appl Surf Sci* 290:267–273
34. Carabineiro SAC et al (2015) Gold supported on metal oxides for volatile organic compounds total oxidation. *Catal Today* 244:103–114
35. Inyawilert K et al (2014) Ultra-rapid VOCs sensors based on sparked-In₂O₃ sensing films. *Sens Actuators B: Chem* 192:745–754
36. Mori M et al (2014) Influence of VOC structures on sensing property of SmFeO₃ semiconductive gas sensor. *Sens Actuators B: Chem* 202:873–877
37. Yan H et al (2015) CuO nanoparticles fabricated by direct thermo-oxidation of sputtered Cu film for VOCs detection. *Sens Actuators B: Chem* 221:599–605
38. Piumetti M et al (2015) Mesoporous manganese oxides prepared by solution combustion synthesis as catalysts for the total oxidation of VOCs. *Appl Catal B* 163:277–287
39. Castaño MH et al (2015) Cooperative effect of the Co–Mn mixed oxides for the catalytic oxidation of VOCs: influence of the synthesis method. *Appl Catal A: General* 492:48–59
40. Abdelouahab-Reddam Z et al (2015) Platinum supported on highly-dispersed ceria on activated carbon for the total oxidation of VOCs. *Appl Catal A: General* 494:87–94
41. Qian X et al (2016) Carbon quantum dots decorated Bi₂WO₆ nanocomposite with enhanced photocatalytic oxidation activity for VOCs. *Appl Catal B: Environ* 193:16–21
42. Itoh T et al (2016) Analysis of recovery time of Pt-, Pd-, and Au-loaded SnO₂ sensor material with nonanal as large-molecular-weight volatile organic compounds. *Sens Mater* 28(11):1165–1178
43. Chen Y, Li X et al (2016) UV activated hollow ZnO microspheres for selective ethanol sensors at low temperatures. *Sens Actuators, B Chem* 232:158–164
44. Xu X et al (2017) Highly sensitive VOCs-acetone sensor based on Ag-decorated SnO₂ hollow nanofibers. *J Alloy Compd* 703:572–579
45. Ueda T et al (2017) Enhanced sensing response of solid-electrolyte gas sensors to toluene: role of composite Au/metal oxide sensing electrode. *Sens Actuators, B Chem* 252:268–276
46. Kaur N et al (2018) Branch-like NiO/ZnO heterostructures for VOC sensing. *Sens Actuators B: Chem* 262:477–485
47. Zhang B et al (2018) Room temperature NO₂ gas sensor based on porous Co₃O₄ slices/reduced graphene oxide hybrid. *Sens Actuators B: Chem*
48. Behera B, Chandra S et al (2018) Synthesis of WO₃ nanorods by thermal oxidation technique for NO₂ gas sensing application. *Mater Sci Semicond Process* 86:79–84
49. Gu F et al (2019) Atomically dispersed Pt (II) on WO₃ for highly selective sensing and catalytic oxidation of triethylamine. *Appl Catal B: Environ* 256:117809
50. Wang L et al (2019) Directly transforming SnS₂ nanosheets to hierarchical SnO₂ nanotubes: towards sensitive and selective sensing of acetone at relatively low operating temperatures. *Sens Actuators B: Chem* 292:148–155
51. Qu F (2019) Fe₂O₃ nanoparticles-decorated MoO₃ nanobelts for enhanced chemiresistive gas sensing. *J Alloy Compd* 782:672–678
52. Chava RK (2019) Fabrication of aggregated In₂O₃ nanospheres for highly sensitive acetaldehyde gas sensors. *J Alloy Compd* 772:834–842
53. Dissanayake S (2020) Mesoporous Co₃O₄ catalysts for VOC elimination: oxidation of 2-propanol. *Appl Catal A: General* 590:117366
54. Marin Figueredo MJ et al (2020) Cerium–copper–manganese oxides synthesized via solution combustion synthesis (SCS) for total oxidation of VOCs
55. Ramanavičius S et al (2020) Selectivity of tungsten oxide synthesized by sol-gel method towards some volatile organic compounds and gaseous materials in a broad range of temperatures 2213(3):523
56. Mousavi H, Mortazavi Y, Khodadadi AA, Saberi MH, Alirezai S (2021) Enormous enhancement of Pt/SnO₂ sensors response and selectivity by their reduction, to CO in automotive exhaust gas pollutants including CO, NO_x and C₃H₈. *Appl Surf Sci* 546:149120

57. Noh YG, Seo H (2021) Improving graphene gas sensors via a synergistic effect of top nanocatalysts and bottom cellulose assembled using a modified filtration technique. *Sens Actuators, B Chem* 334:129676
58. Anand R, Chawla P (2016) A review on the optimization techniques for bio-inspired antenna design. In: 3rd international conference on computing for sustainable global development (INDIACom). IEEE, pp 2228–2233
59. Srivastava A, Gupta A, Anand R (2021) Optimized smart system for transportation using RFID technology. *Math Eng Sci Aerosp (MESA)* 12(4)
60. Juneja S, Juneja A, Anand R (2019) Reliability modeling for embedded system environment compared to available software reliability growth models. In: International conference on automation, computational and technology management (ICACTM). IEEE, pp 379–382
61. Kirubasri G, Sankar S, Pandey D, Pandey BK, Singh H, Anand R (2021) A recent survey on 6G vehicular technology, applications and challenges. In: 9th international conference on reliability, Infocom technologies and optimization (trends and future directions) (ICRITO). IEEE, pp 1–5

High-Impedance Surface Backed Circular Patch Antenna for Wireless Communications



Akash Kumar Gupta, P. Satish Rama Chowdary, and M. Vamshi Krishna

Abstract A multi-band antenna is a very attractive solution for wireless communication applications. A low-profile miniaturized compact circular patch antenna backed with a high-impedance surface antenna is presented in this work. A high-impedance surface-based ground plane is an effective method for suppressing the surface waves and hence improves the performance of a patch antenna. The HIS-based ground plane is designed on Fr-4 substrate with a rectangular patch of dimensions of 10 mm \times 10 mm having protrusion at the center of the patch. A circular microstrip patch antenna is designed on Fr-4 substrate, and its performance is compared with metallic ground plane and HIS ground plane. The circular patch antenna backed with HIS ground plane radiates in multiple bands 1.63–1.66, 3.86–4.03, 4.19–5.12 GHz with bandwidths of 3–5% in all bands.

Keywords Circular microstrip patch · High-impedance surfaces · Multi-band

1 Introduction

Efforts to fulfill the severe needs of new and diversified antenna technologies and communication services necessitate an unrelenting effort in antenna designing. The most used microstrip patch antennas suffer from surface waves. The surface waves in antennas are undesirable because they propagate along the ground plane and do not radiate to free space. There is a decrease in the antenna's directivity, gain, and efficiency [1–12]. Surface waves are excited on microstrip antennas when the

A. K. Gupta (✉)

Department of ECE, Centurion University of Technology and Management, Gajapati, Odisha, India

e-mail: akgupta452@gmail.com

A. K. Gupta · P. Satish Rama Chowdary

Department of ECE, Raghu Institute of Technology, Visakhapatnam, India

e-mail: satishchowdary@ieee.org

M. Vamshi Krishna

Department of ECE, Dhanekula Institute of Engineering and Technology, Vijayawada, India

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023

235

S. C. Satapathy et al. (eds.), *Computer Communication, Networking and IoT*,

Lecture Notes in Networks and Systems 459,

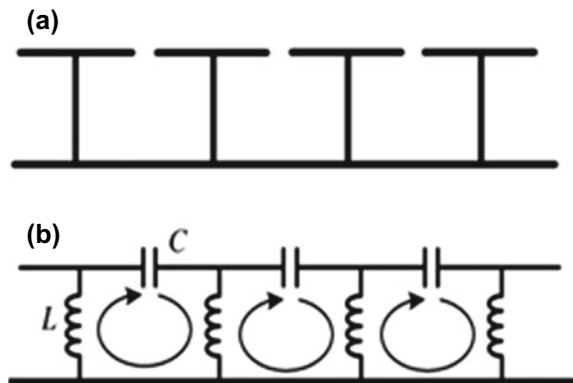
https://doi.org/10.1007/978-981-19-1976-3_30

substrate's permittivity is greater than 1. Surface waves also contribute to the mutual coupling between array elements and result in end-fire radiation. When these waves are shot into the substrate, they are discharged at an elevation angle of about $\pi/2$ and $\sin^{-1}\left(\frac{1}{\sqrt{\epsilon_r}}\right)$. After being reflected from the ground plane, these waves are also reflected from the dielectric-air interface. The end-fire radiation is created by the reflection and diffraction of these surface waves along the borders of the microstrip structure.

Many methods for reducing the surface waves generated by printed antennas have been developed during the last few decades. For example, adding a second dielectric layer on top of the patch [6] or tweaking the patch's form [7] are two options. To get a low effective dielectric constant, one must drill an air cavity underneath the patch. On substrates with high dielectric constants, compact circuit design can be realized. Reduced surface waves are caused by a rise in the dielectric constant [9], but this also reduces the bandwidth, and increasing substrate thickness is one solution to this problem. Surface waves generated by a high and thick permittivity substrate can be suppressed by utilizing EBG, which has a stopband around the target frequency [11]. This wave is made up of the substrate's TM and TE modes, respectively. Waves along the transverse direction are attenuated and have a true propagation constant above the cut-off frequency in these two modes [12]. Substrates h and r have a significant impact on the phase velocity of surface waves. A waveguide EBG (PBG) structure is shown in Fig. 1b preventing the propagation of a surface wave.

The paper has been organized into four sections in which Sect. 1 introduces HIS, Sect. 2 describes the HIS structure, Sect. 3 focuses on the design and implementation of the circular patch over a HIS ground plane, and Sect. 4 investigates the result.

Fig. 1 a High-impedance surface structure. b HIS equivalent circuit



2 High-Impedance Surface Structures

According to optics, the photonic bandgap (PBG) inspired the HIS [13]. To create pass or stopbands, the HIS periodic structure has been used over a microwave planar waveguide. The HIS surface in the shape of mushroom (with protrusions) has been detailed in [14], while the uniplanar EBG surface (without vias) has been explained in [15]. However, the manufacturing process has been made easier, but the EBG is less sensitive to polarization and incidence angle polarization. To obtain a broad range of bandwidth, lower frequency, and a smaller dimension than the uniplanar HIS, a mushroom-like HIS surface is ideal. Antenna performance may be improved by the characteristic of surface wave suppression, which reduces backward direction and the amount of power that is lost. Increasing the radiation efficiency of an antenna, dual-band HIS structures with vias must be designed for multi-band applications, however, manufacturing is more difficult. Changing the height and position of the vias results in a dual bandgap. According to the literature, several triple-band HIS configurations have also been proposed. The fabrication, on the other hand, is an essential consideration that is influenced by the number of pins vias, HIS size, and HIS location. There is no stop band frequency in HIS without vias.

A two-dimensional mushroom-shaped HIS design was introduced by Anguera et al. [16]. The design includes four components: metallic ground plane, dielectric material, metallic patches, and protrusion vias. These HIS designs provide a unique stopband characteristic for surface wave propagation. To explain the HIS structure working, an equivalent model of design is used which consists of an LC filter array [14]. The inductor L effect is caused by the current passing through vias, whereas the capacitance C effect is caused by the distance between adjacent patches. s stands for the gap, whereas t stands for the substrate thickness, and r represents the dielectric constant. It is possible to reduce the bandgap by increasing the capacitance or inductance, which is based on the central frequency.

$$L = \mu_o t \tag{1}$$

$$C = \frac{W\epsilon_0(1 + \epsilon_0)}{\pi} \cosh^{-1} \left(\frac{2W + s}{s} \right) \tag{2}$$

$$f = \frac{1}{2\pi\sqrt{LC}} \tag{3}$$

$$BW = \frac{\Delta f}{f_c} = \frac{1}{\eta} \sqrt{\frac{L}{C}} \tag{4}$$

3 Design of Circular Patch Antenna on HIS

HIS structure designed with metallic ground plane followed by FR4 substrate having a dielectric constant of 4.4 and loss tangent of 0.019 of height 1.6 mm is used. For HIS structure, a rectangular patch of 10 mm \times 10 mm with metallic via at center is used. The HIS ground plane is picturized in Fig. 2. The gap between adjacent patches is chosen 0.25 mm for good stop band response. A circular patch antenna is intended

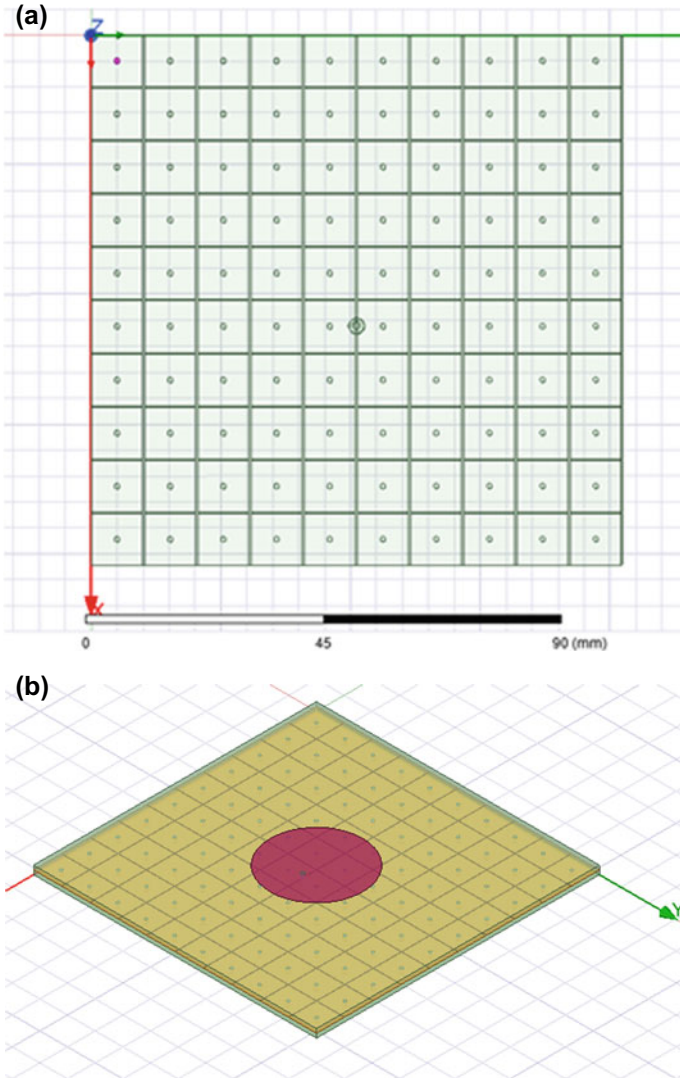


Fig. 2 a HIS with rectangular patch array. b Circular patch antenna on HIS backed ground plane

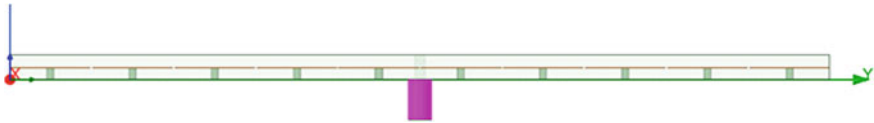


Fig. 3 Cross-sectional view of HIS-based circular patch antenna

Table 1 Design parameters

Design parameter	Dimensions in mm
Ground plane length	104.5
Ground plane width	104.5
HIS patch dimensions	10 × 10
HIS array size	10 × 10
Via diameter	1
Substrate height	1.6
Circular patch radius	17

to work at 2.4 GHz. The circular patch is placed over a substrate of height 1.6 mm over the HIS-based ground plane. The designed circular patch antenna is picturized in Fig. 2b. The patch is excited with a coaxial feed (Fig. 3).

The design parameters are tabulated (Table 1).

4 Results

The antenna design, implementation and simulation are carried out in Ansys Electromagnetics Suite and the results are discussed following sections. The designed HIS-based circular patch antenna investigated for major parameters like return loss, radiation pattern, gain, and current density.

4.1 Optimization and Effect of the Gap

To obtain the optimum gap between HIS patches parametric analysis is performed for different gap values 0.25–1 mm. Hence, with analysis response gap is optimized to $g = 0.5$ mm. The response is shown in Fig. 4.

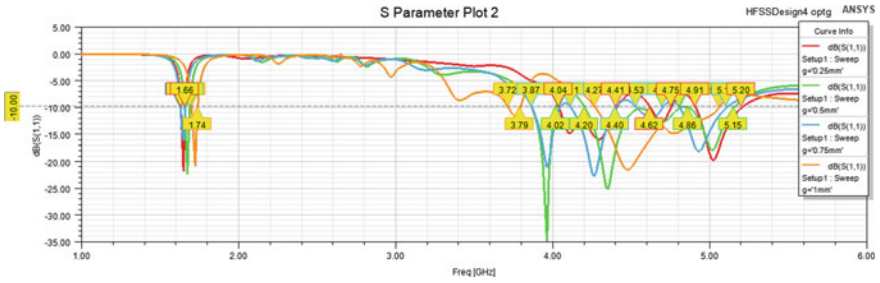


Fig. 4 Plot for return loss for $g = 0.25, 0.5, 0.75, 1$ mm

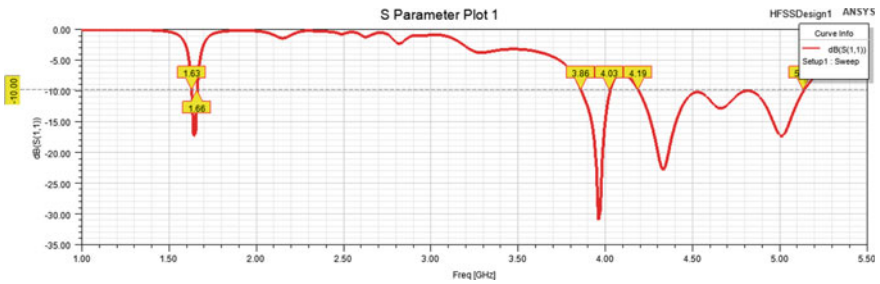


Fig. 5 Return loss plot

4.2 Return Loss

Return loss is a measure of reflected power. For a good antenna, performance return loss must be less than -10 dB. From the S11 plot, the antenna is resonating at 1.63–1.68, 3.86–4.03, 4.19–5.20 GHz. with a maximum dip at -31.0 dB (Fig. 5).

4.3 Radiation Pattern

The antenna has a good radiation pattern in forward direction and very low radiation in a backward direction. The radiation pattern is shown in Fig. 6.

4.4 Gain

The gain plot is shown in Fig. 7. The gain plot shows the maximum gain of 4.38 dB at the desired frequency.

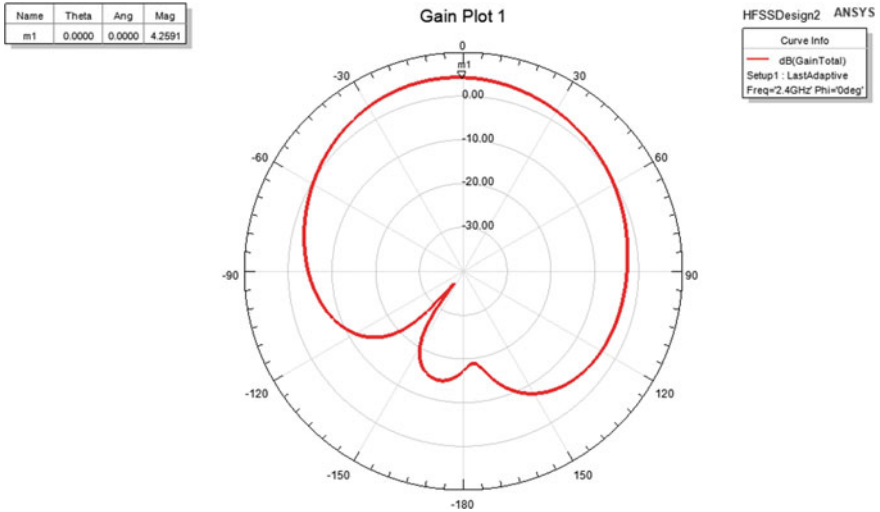


Fig. 6 Radiation pattern

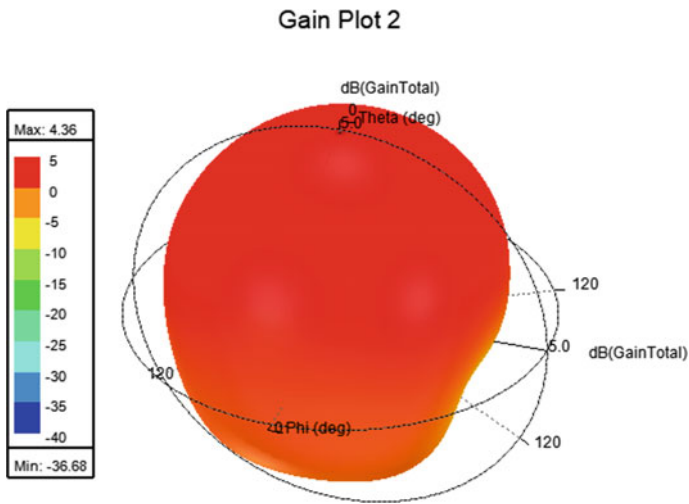


Fig. 7 3D gain plot

4.5 Current Density

The current density distribution shows a vector or current distribution along with the excited patch. It has shown maximum current is at pin of probe feed and reduces sinusoidally along the patch surface (Fig. 8).

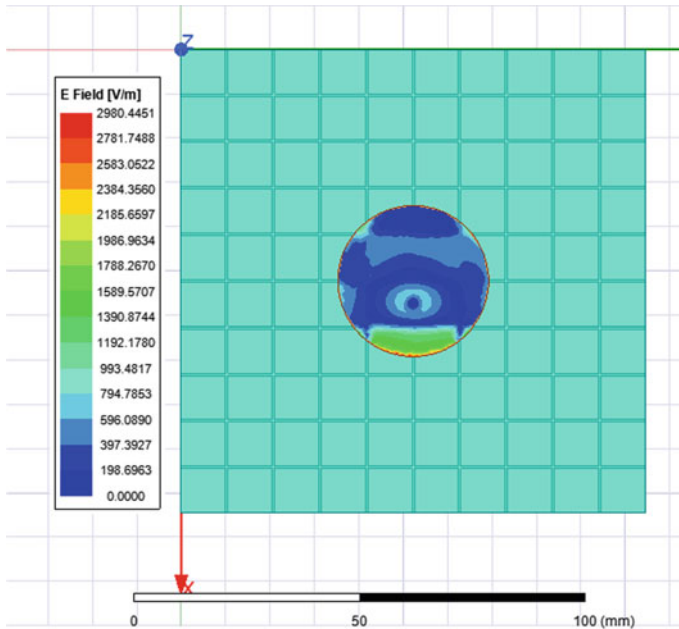


Fig. 8 Current distribution over the circular patch

5 Conclusion

In this work, circular patch antenna with metallic ground plane and HIS plane are investigated. In the metallic-based ground plane, there are surface waves radiation which causes a reduction in gain and more spill over in radiation pattern. While the use of HIS backed ground plane, the surface waves will be reduced and hence the gain can be improved. The structure of the HIS can help to prevent surface waves and power leakage. Gaps, which operate as filters, prevent the flow of current from reversing back to it to substrate with same phase from the results, and it is observed that the return loss at desired operating frequency is improved and as the antenna's bandwidth is also when HIS ground plane is used. The designed circular patch antenna has the multi-band response from 1.63 to 1.66, 3.86 to 4.03, 4.19 to 5.12 GHz with bandwidths of 3–5% in all bands.

References

1. Attiah et al (2019) Independence and fairness analysis of 5G mm-wave operators utilizing spectrum sharing approach. *Mob Inf Syst* 201:12
2. Attiah ML et al (2019) A survey of mm wave user association mechanisms and spectrum sharing approaches: an overview, open issues and challenges, future research trends. *Wirel Networks* 1–28

3. Mohsen et al (2018) Control radiation pattern for half width microstrip leaky wave antenna by using PIN diodes. *Int J Electr Comput Eng* 8(5)
4. Wong SW et al (2007) EBG-embedded multiple-mode resonator for UWB bandpass filter with improved upper-stopband performance. *IEEE Microw Wirel Compon Lett* 17(6):421–423
5. Qian et al (1999) A microstrip patch antenna using novel photonic band-gap structures. *Phys Rev* 66(6):1–4
6. Alexópoulos et al (1984) Fundamental superstrate (cover) effects on printed circuit antennas. *IEEE Trans Antennas Propag* 32(8):807–816
7. Jackson DR et al (1993) Microstrip patch designs that do not excite surface waves. *IEEE Trans Antennas Propag* 41(8):1026–1037
8. Yook JG et al (2001) Micromachined microstrip patch antenna with controlled mutual coupling and surface waves. *IEEE Trans Antennas Propag* 49(9):1282–1289
9. Weile DS (2013) Electromagnetic band gap structures in antenna engineering. *IEEE Antennas Propag Mag* 55(6):152–153
10. Abdulhameed et al (2018) Controlling the radiation pattern of patch antenna using switchable EBG. *TELKOMNIKA Telecommun Comput Electron Control* 16(5):2014–2022
11. Abdulhameed MK et al (2018) Improvement of microstrip antenna performance on thick and high permittivity substrate with electromagnetic band gap. *J Adv Res Dyn Control Syst* 10(4):661–669
12. Singh N et al (2010) Effect of photonic band gap structure on planar antenna configuration. In: *MMS 2010: proceedings 10th mediterranean microwave symposium, North Cyprus*, pp 81–85
13. Yablonovitch E (1994) Photonic crystals. *J Mod Opt* 41(2):173–194
14. Gupta AK et al (2021) DGS-based T-shaped patch antenna for 5G communication applications. In: Chowdary P, Chakravarthy V, Anguera J, Satapathy S, Bhateja V (eds) *Microelectronics, electromagnetics and telecommunications. Lecture notes in electrical engineering*, vol 655. Springer, Singapore. https://doi.org/10.1007/978-981-15-3828-5_2
15. Sievenpiper et al (1999) High-impedance electromagnetic surfaces with a forbidden frequency band. *IEEE Trans Microw Theory Tech* 47(11):2059–2074
16. Anguera J, Andújar A, Jayasinghe J, Chakravarthy VVSS, Chowdary PSR, Pijoan JL, ... Cattani C (2020) Fractal antennas: an historical perspective. *Fractal Fractional* 4(1):3

A Critical Analysis on Attacks and Challenges in VANETs



Y. Sarada Devi and M. Roopa

Abstract Vehicular ad hoc networks (VANETs) are developing kind of MANETs with strong applications in ITS. VANETs have been considered a dominant courtesy from the community of research under wireless communication and have gained a site as one of the most projecting research areas in intelligent transportation system, with a mark to provide safety on roads and precautions for passengers. In the world, the concentration of traffic is growing leading to mobbing, bad fates and contamination. Vehicular ad hoc network, a sub-class of mobile ad hoc network, is presented as a solution to accomplish the problem of these issues. VANET is ahead with consideration among scholars with its huge variety of applications in the field of ITS. The broadside emphasises on encounters and security attacks in VANET.

1 Introduction

VANET has given better quality of experiencing a safe drive. Those linked to Internet must be trusty and safe. VANETs mainly focus on the approach of MANETs. The difference in speed of nodes is main alteration in MANET and VANET protocols. Many expressions state the technology of VANETs like vehicle to vehicle and vehicle to infrastructure [1].

These are kind of mobile ad hoc network with routes of road, with intention to offer traffic security, progress traffic flow and improve the driving skills. It depends on transport authority for record keeping and handling the Road Side Units (RSUs) and On-Board Units (OBUs) [2]. An OBU is connected in each automobile like source to connect with other vehicles, while RSUs are fitted sideways with network systems. RSUs are helpful in communicating with the infrastructure and have devices in network for dedicated short-range communication (DSRC) [3] (Fig. 1).

Y. S. Devi (✉) · M. Roopa
Department of ECE SRM Institute of Science and Technology, Ramapuram, Chennai, India
e-mail: sy9149@srmist.edu.in

M. Roopa
e-mail: roopam@srmist.edu.in

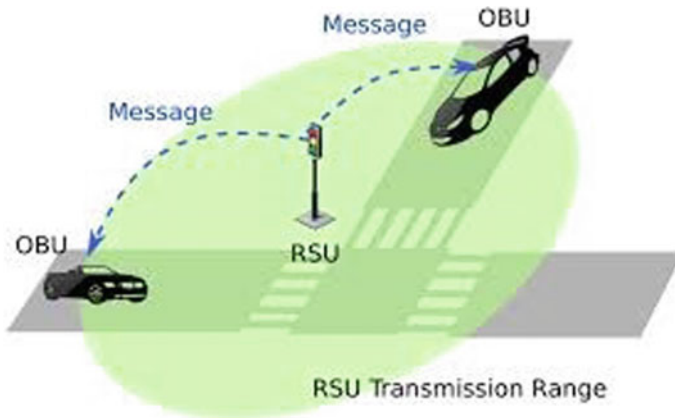


Fig. 1 VANET modules

VANETs constitute two types: Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. In the V2V, vehicles can get connected with each other to make a discussion on data related to traffic. In the V2I, vehicles can directly get linked with the infrastructure to have interchange about information relate to traffic. Announcement amid unlike nodes can be done by using wireless protocol DSRC[3]. Establishing a less cost system was likely to happen because of blend of GPS technology and DSRC, and making use of this is possible only of another vehicle is also equipped with the same. Several countries are under process to use VANETs and make use of this technology to get executed everywhere (Fig. 2).

Also, in this technology, integrity must be guaranteed to all the messages like route prediction, route discovery and traffic analysis that are being transmitted between all the vehicles that work under the principle of VANTEs. By providing this integrity,

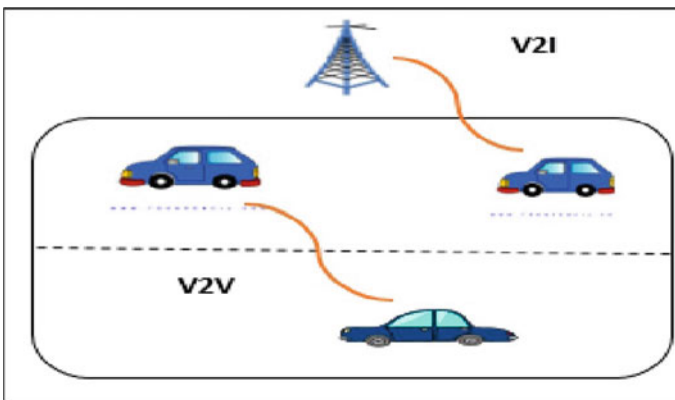


Fig. 2 Vehicle to vehicle and vehicle to infrastructure

the road life can be made free from accidents, and of course emergency situation can be handled easily. VANETSs provide a potential to promise the vehicles safety with dealings including interference assistance, safety warning of blind spot, weather, collision caution, etc. Drivers can be notified with the messages about the speed of the vehicles and can be made alert.

Transit operation and ride sharing are dynamic enticements of VANETs that can make vehicles not only to communicate with vehicle but also with the driver. Due to the presence of large network, it will be very difficult to verify each node in less time, which may lead to accidents. Increase in count of vehicle also leads to increase in bandwidth which may lead to interference of signals. However, it being a network, it is weak to attackers who can disturb the messages or can insert some hateful data. Security must be the main alarm in employment of VANETs. The main tests being faced by VANETs are attacks, flooding, spamming and malwares. VANETs are time dependent. Messages can be hindered during transmission due to jammers which decreases the performance of VANETs. Numerous trials can be taken over to plan endangered VANETs. Sanctuary and confidential issues must be touched effectively to apply the VANETs, by scheming a cultured procedure that will handle all classes of threats and attacks. To lecture these matters, numerous revisions have projected the connected verification and confidentiality schemes.

2 Characteristics of VANET

VANETs are the wireless networks with nodes fixed on the road side units or the vehicles with high mobility. This network is extremely energetic, dependable, and provides multiple services. The main characteristic is the limited access to the network infrastructure [4].

The characteristics of VANET are conferred below.

- **Mobility:** The key structures of VANETs are its high mobility nodes. The mobility of these nodes are high when compared with MANETs. Earlier many theories have discovered this characteristic. Because the nodes have high mobility, they can communicate in less time in the network.
- **Wireless:** As the connection and communication are done in a wireless medium, it is always necessary to establish a secure medium.
- **Network Topology:** The topology of the network is not fixed. It changes with respect to time and with movement of vehicles. This property of VANETs makes them more exposed to attacks and difficult to identify the doubtful vehicles.
- **Safety:** VANETs can expand safety of driver, improve passenger luxuries and progress the flow of traffic. The key benefit is that vehicles can connect straight, which allows the number of applications that need direct communication between nodes to other networks like RSUs or OBUs.
- **Transmission Power:** VANETs have very controlled power of transmission that varies between 0 and 28.8 dBm. It is restricted to the range of 1 km.

Table 1 Characteristics of VANETs

Characteristics	VANET
Topology	Active and flexible
Infrastructure	Required less infrastructure
Safety and QOS	Less
Speed	High
Cost	Less
Existence time	Less
Route selection and maintenance needed	Difficult
Network strength	High
Relay equipment	Wireless nodes
Network features	Low capacity and errors are sometimes high

- **Network Strength:** The network strength purely is based on traffic flow.
- **Instability:** Connections between the nodes are established because of their movement in VANETs. Connection between the vehicles can be lost at any time due to mobility of vehicles, and of course security assurance can be difficult (The characteristics can be as shown in Table 1).

VANETs’ SECURITY AND ATTACKs’

- **Security Services**

In VANETs, the safety ensures that the moved data is not changed by invaders. In addition to that, the driver him/herself is responsible to let to know the traffic conditions in the given time. VANETs are more immune to attacks due to their characters. It is quite important that security issues are pointed correctly, else it may lead to create many issues for secure and safe communication. For a VANET to be secure, it is important that the requirements are properly mentioned for the network to function appropriately. If the requirements are not met properly, it may lead to attacks. The security needs in VANETs are classified into five categories: availability, confidentiality, authentication, data integrity and non-repudiation. A break in the communication link may be because of the vehicles moving in the opposite direction and this can be limited to fraction of seconds. The entire VANET can be disturbed if then attacker interrupts in middle when a safe message is being broadcasted in an open access medium. These kinds of issues make the network get exposed to various attacks.

The attackers are categorised into four varieties in VANETs[5] (Fig. 3).

- (i) **Insider versus outsider attackers:** The insider attacker is the genuine operator with good information about configuration of the network. The outside attackers are not real users, with imperfect ability to attack the network.

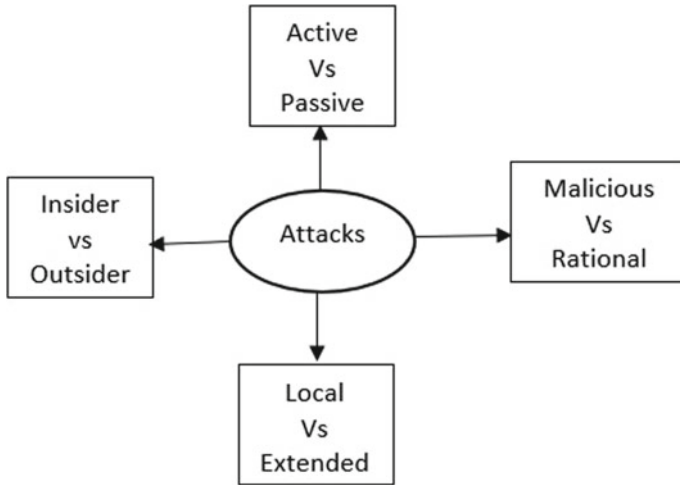


Fig. 3 Classification of attacks in VANETs

- (ii) **Active versus passive attackers:** Active attackers either create forged communications or do not transmit received messages, while passive attackers are not involved in the statement.
- (iii) **Malicious versus rational attackers:** Among these two, the first one destroys the nodes without any personal interest, whereas the second one does it for personal benefit.
- (iv) **Local versus extended attackers:** Limited resources are used by the local attackers, whereas resources are fully utilised by extended attackers.

To deliver safe communication, a data of threats and attacks is needed to challenge all security issues. In this section, the threats and attacks on each security service in VANETs will be discussed.

- **Attacks**

Obtainability of data is actually significant portion of the VANET, without which efficiency will be decreased [6, 7].

- **DOS (Denial of Service) Attacks:**

DOS is one of the utmost communal attacks in VANETs. This is because of the vehicles that are internal or external causing the attacks. There will be many possible ways for the attacker to jam the signal in this attack. Many attackers can cause disturbance to the signal simultaneously in a distributed way, and it is called distributed denial of service (DDoS) [8].

- **Jamming Attack:**

A communication channel is distributed in the network with the help of a highly powered signal with equal frequency. A valid safety alert is not maintained in this attack which make this most dangerous one.

- **Malware Attack:**

This is the attack that generally happens by taking help of software into the system by RSU and OBU. There is a chance for entire system to get corrupted because of this attack.

- **Broadcast Tampering Attack:**

This attack makes the duplicate messages to be generated by unreliable vehicles in the network. Because of this, there is a chance for new messages to get introduced into the network. This can result to hiding of real information and may lead to accidents.

- **Blackhole Attack:**

Targets availability is the main feature of this attack. This is generally raised because of the registered user. The assumed node accepts the packets from the network but it drops the influence in the interacting process. This will disturb the routing table and stops a significant note to the addressees due to the malevolent node, which imagines to donate in the non-practical occasion.

- **Grey hole Attack:**

It is asymmetrical to that of the blackhole attack. It occurs when dishonest automobiles choose few of the data packets to forward and dropping the other packet without being followed.

- **Greedy Behaviour Attack:**

This is because of the functioning of the authentication code. When the MAC protocol is misused by the spam vehicles, the bandwidth will be increased and this will increase the cost to the other vehicles. This will result in excess traffic and lead to crash on the broadcast channel, and a delay is produced in the amenities of the listed user.

- **Spamming Attack:**

In this attack, a large volume of junk message is inserted by the attacker. Additional bandwidth may be used to crash the messages. Some certificates and keys are used to provide confidentiality to the messages transmitted through messages and this is guaranteed through cryptography.

- **Eavesdropping Attack:**

This is a very common attack that generally appears in wireless networks whose goal is to hold the personal information from protected data.

- **Traffic Analysis Attack:**

This can be termed as a hazardous attack that hovers confidentiality. Here, the frequency is analysed after attending to the message and the message is mined.

- **Man-in-the-Middle Attack:**

This attack can happen in the middle of vehicle-to-vehicle communication. This attack will closely check the messages and change them. Because of this, it is like the attacker can access and control the entire network.

- **Social Attack:**

This attack is mainly to divert the attention of the driver. The invader conveys out corrupt and unprincipled posts to the drivers. It therefore affects the driving knowledge and routine of the automobile in the network.

- **Attack on Authentication**

Validation is a vital portion in the VANET system, which can be used to defend the attacks due to the malevolent nodes incoming the system. The certification is accountable for shielding VANETs from all varieties of attacks.

- **Sybil Attack:**

In this attack, fake identities are produced by the attacker by generating false IDs. There is also a chance for manipulating the behaviour of the vehicles.

- **Tunnelling Attack:**

This is mostly similar to the wormhole attack. The attacker customs the similar network to start the isolated talk, and there is a chance that two vehicles which are far away can communicate if they are near creating a false information.

- **GPS Spoofing:**

False GPS locations are created by the attacker to make the driver feel that the vehicle is in some other location.

- **Node Impersonation Attack:**

The valid ID of the registered users in the network is guessed by the attacker.

- **Free-Riding Attack:**

False authentication messages are created by the attackers while being cooperative in the network. Here, the hateful operator may take benefit of additional operator's confirmation without using its own. This kind of act is free-riding attack.

- **Replay Attack:**

This playback attack happens when lawful data is falsely conveyed or root a suspension to yield an unofficial and malevolent effect. Large memory is required by the network to handle this attack.

- **Key and/or Certificate Replication Attack:**

Creation of duplicate keys or certificates is the reason for this attack. This mainly creates uncertainty making situation worse for the traffic.

- **Message Tampering:**

It is a very mutual attack, in which the invader can modify the swapped posts in vehicle-to-vehicle or vehicle-to-infrastructure communication.

- **Masquerading Attack:**

Incorrect IDs are taken to perform as other vehicle. This attack happens when operator will not use individual uniqueness and fantasises to be a different user to lawfully gain unsanctioned contact.

3 Challenges and Future Perspectives

Assumed the tasks and features of VANETs, few standpoints must be measured to project new competent message tactics [9]:

- **Network Management:**

Due to continuous change in the network architecture, the topology continuously changes. Maintenance of structures like tree cannot be done easily as it is difficult to maintain such huge topologies.

- **Congestion and collision Control:**

The size of the network is also a challenge. Due to the unpredicted nature of the network and its topology maintain, traffic in urban and rural areas in different periods of time in a day still remains as a challenge.

- **Environmental Impact:**

Electromagnetic waves which are used as a means of communication in this network may get disturbed by the environment during propagation.

- **MAC Design:**

Shared medium is used in VANET to establish communication which requires MAC design.

- **Security:**

Security measures are to be satisfied as this network is mainly designed for road applications.

- **Real time Constraint:**

VANET topology is dependent on time. Delay is not an appreciable factor in transmission of messages. So fast algorithms are to design to achieve truthful goals.

- **Data Consistency Liability:**

Accountability and correlation are maintained between transmitter and receiver to avoid inconsistency in the network to improve the performance of the network.

- **Low tolerance for error:**

Small errors during transmission can also cause harm to the entire network as there can be some critical information that has to be transmitted in a very small duration.

- **Key Distribution:**

Since some encryption standards are adopted every message has to be encrypted and decrypted with the corresponding keys. So, design of key is an important factor.

- **Incentives:**

Productions of vehicles with this VANET architecture are gaining good interest among the consumers. Therefore, fruitful placement of vehicular networks will entail motivations for producers, patrons and management.

- **Highly heterogeneous vehicular networks:**

Huge variety of wireless systems is being developed these days which is establishing a connectivity across different networks. Accordingly, it is probable that the subsequent group of ITS replicates a good full method to network (Fig. 4).

- **Localization systems:**

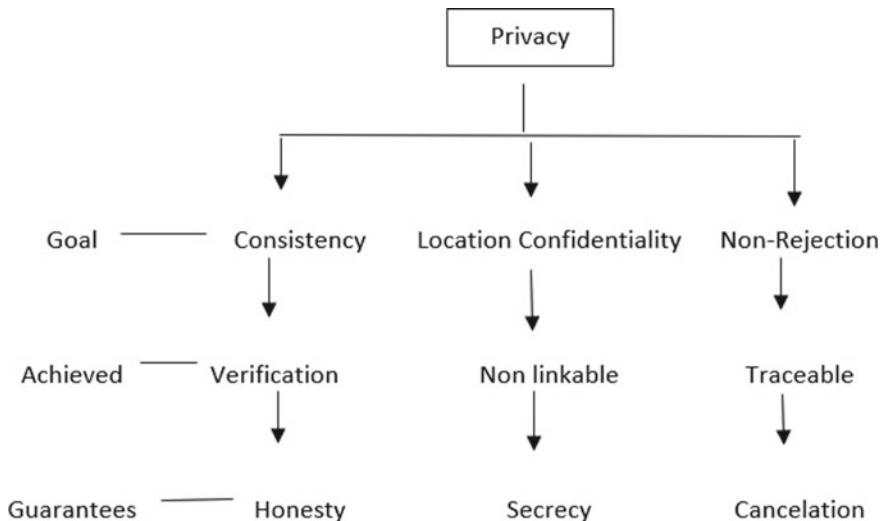


Fig. 4 Catalogue of privacies in VANETs

More genuine and accurate systems are to be designed to handle critical situation in VANETs. A good solution is to entrench an efficient navigation system.

- **Disruptive tolerant communications:**

Problematic issues like delay in propagation and less reliability in transmission of data are to be addressed in the designs. To improve the performance of the system, some special techniques can be introduced. These glitches may be resolved/diminished sightseeing novel communication tactics for Heterogeneous Networks.

- **Tracking a target:**

To establish the communication in the network is a key factor in any network. When the information is to be transmitted between vehicles, it should be seen that a proper link is established between both, and this link will not get detached. Hence, it is necessary that vehicles should be tracked continuously. Special tracking devices are also to be introduced into the system which can serve this purpose.

4 Applications of VANETs

The RSU is to be preserved in place of an entree point or router or even a barrier point that will stock statistics and deliver statistics when required. Entire information on the RSU will be uploaded or downloaded by vehicles. VANETs sustain an extensive variety of applications since modest one hop data distribution to multi-hop distribution of posts on massive distance [10–14].

Sample applications of VANETs:

- Automated power-assisted brake lights that permit a motorist to respond to vehicles breaking yet they are covered.
- Platooning that lets vehicles to trail a principal vehicle by receiving the information about the vehicles and making them electronically attached.
- Information structures that make use of VANET announcement to up-to-date data about the hindrances using GNS
- Emergency services in which safety and status data is provided to decrease the delay and to increase the speed if emergency rescue operations.
- On the road services are those being developed to provide wireless information on the highways.

5 Conclusion

In an ITS, VANETs are measured as additional energetic and auspicious research zone because of its exclusive features; consequently, safety and confidentiality are measured as serious topics. The objective of VANET is to guarantee the protection

of human on the road by propagating protective posts amid the automobiles and also deliver ease facilities to the travellers. The protection posts are disseminated in an exposed situation because of which VANETs are further susceptible to attacks. Consequently, a cultured and vigorous safety procedure has to be planned to challenge hazardous safety and confidential attacks. This paper mainly tried to focus on different aspects like challenges, attacks and applications of VANETs.

References

1. Javed MN et al (2019) VANET's security concerns and solutions: a systematic literature review. In: Proceedings of the 3-rd international conference on future networks and distributed systems (ICFNDS) ACM, July 1–2, pp 1–12
2. Abu Talib M et al (2018) Systematic literature review on internet-of-vehicles communication security. *Int J Distrib Sensor Netw* 14(12). ISSN: 1550147718815054
3. Cui J, Wei L, Zhang J, Xu Y, Zhong H (2019) An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. *IEEE Trans Intell Transp Syst* 20(5):1621–1632
4. Lu Z, Qu G, Liu Z (2019) A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans Intelligent Transport Syst* 20(2):760–776
5. Jafer M et al. (2019) Secure communication in VANET broadcasting. *ICST Trans Secur Safety* 5(17)
6. Cui J, Wei L, Zhang J, Xu Y, Zhong H (2019) An efficient message authentication scheme based on edge computing for vehicular ad hoc networks. *IEEE Trans Intell Transp Syst* 20(5):1621–1632
7. Hussain R, Hussain F, Zeadally S (2019) Integration of VANET and 5G security: a review of design and implementation issues. *J Future Gener Comput Syst* 843–864
8. Deshai N, Sekhar BVDS, Reddy PVGD, Chakravarthy VVSSS (2020) Processing real world datasets using big data hadoop tools. *J Scientif Indust Res (JSIR)* 79(7):631–635
9. Avinash S et al (2019) Implementing security services in VANET using cryptography based on artificial neural network. *J Comput Mathem Sci* 10(9):1573–1584
10. Venkataramana S, Sekhar BVDS, Deshai N, Chakravarthy VVSSS, Rao SK (2019) Efficient time reducing and energy saving routing algorithm for wireless sensor network. *J Phys: Conf Ser* 1228(1):012002, IOP Publishing
11. Sewalkar P, Seitz J (2019) Vehicle-to-pedestrian communication for vulnerable road users: survey, design considerations, and challenges. *Sensors* 19:358
12. Lu Z, Qu G, Liu Z (2019) A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans Intell Transp Syst* 20:760–776
13. Ali I, Hassan A, Li F (2019) Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey. *Veh Commun* 16:45–61
14. Murali K, SivaPerumal S (2021) Sector multi-beam space optimal bit error rate enhancement in wireless 5G using power domain NOMA. *Soft Comput.* <https://doi.org/10.1007/s00500-021-05879-y>

Development of 5G Array Antenna Using 2×1 Power Divider for Enhancing Gain in Wireless Applications



Sreevardhan Cheerla, V. Subbareddy, Syed Noor Mohammad, Moghal Ajarvali, and Nichenamtela Neeraj

Abstract A 2×1 power divider-based antenna array design and analysis is presented in this paper. The antenna array employs a planar substrate with its permittivity of 1.96 and having a thickness of 0.762 mm. The proposed array geometry has antenna elements which are fed using the designed power divider. The typical single element patch has dimensions of (3.153×4.403) mm. In order to avoid the inductive effects, the elements are separated by a distance of 13.522 mm. The simulated antenna is analyzed in terms of S11 and radiation pattern plots. For a better insight, the characteristics of the single element antenna are compared with the respective array configuration.

Keywords Patch antenna · Power divider · Antenna array

1 Introduction

In earlier days, communication had become an important activity for human living, Antennas plays a vital role in wireless communication. Different kinds of antennas are designed as per the required application, i.e., for WLAN, PCS, 3G, 4G, and 5G [1–5]. Higher bandwidth and frequencies had become the major barriers for the latest technology like smartphones, wireless network providers, etc. In 5G technology, the cellular system is shifted to a higher rate to provide the higher bandwidth and frequencies. In 5G the centimeter and millimeter waves provide the higher bandwidth as compared to 4G or 5G. There are different bandwidths allocated to 5G like 3500 MHz, 28 GHz, and 700 MHz. When moved to millimeter waves new challenges take place in antenna designing for base stations and mobile devices [6–10]. However, many challenges exist in using millimeter wave frequencies which include atmospheric absorption, large-scale attenuation of human bodies, propagation loss shadowing and materials, and sensitivity to blockage. To control the above challenges, we need high gain high directional beamforming antennas for both mobile

S. Cheerla (✉) · V. Subbareddy · S. N. Mohammad · M. Ajarvali · N. Neeraj
Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India
e-mail: Sreevardhancheerla@kluniversity.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023
S. C. Satapathy et al. (eds.), *Computer Communication, Networking and IoT*,
Lecture Notes in Networks and Systems 459,
https://doi.org/10.1007/978-981-19-1976-3_32

257

devices and a base station. To overcome the path loss at millimeter wave frequencies the beamforming should be applied.

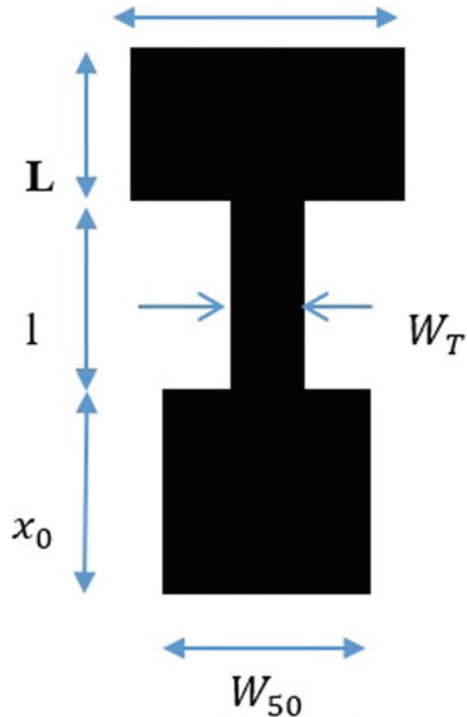
Power dividers (PD) have a reasonable performance in splitting the power as desired requirements especially in the electromagnetic applications. These PDs are used as the most significant part of the feed system in antenna array configurations. This due to the reason that the array configuration often require various varieties of tapping the current while exciting the elements in it. The desired beamforming can be achieved, by controlling power division ratio.

In this paper, a single element patch antenna and two element patch antenna array for 28 GHz operating frequency has been proposed and designed. The significant insight of the work is that when compared to the single element the directivity of the antenna array is enlarged [10, 11].

2 Analysis and Design

The proposed antenna configuration in the basic form is presented in Fig. 1. Usually, the literature suggests to have the larger dimension of the planar patch restricted to half or quarter wave length. It is always interesting to see that the patch antenna

Fig. 1 Geometry of basic antenna



dimensions in terms of its wave length are crucial. In the case of miniaturization or small sized antennas, the corresponding patch may not cooperate for radiation. In such scenarios, the corresponding thickness of the substrate can be manipulated [12].

Fringing fields are obvious through the edges of the patch. These later contribute to the radiation. It is possible to compute the respective E field emerging out in the form of radiation using Eq. (1).

$$E = \theta E_o \cos c \left(\frac{\beta L}{2} \sin \theta \right) \quad (1)$$

The dimensions of the patch antenna are usually related mutually with each other. Hence, taking one particular parameter in to consideration, the other parameters can be easily computed with the relation they have. The following Eq. (2) through Eq. (6) are responsible for the antenna design [2]

The width is mentioned as

$$W = \frac{1}{2f_r \sqrt{\epsilon_o \mu_o}} \sqrt{\frac{2}{\epsilon_r + 1}} \quad (2)$$

The corresponding longer dimension is given using the Eq. (3)

$$L = \frac{12d(\epsilon_{\text{reff}} + 0.3)\left(\frac{W}{h} + 0.264\right)}{\left[(\epsilon_{\text{reff}} - 0.258)\left(\frac{W}{h} + 0.8\right)\right]} \quad (3)$$

The material properties are given as

$$\epsilon_{\text{reff}} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2\sqrt{1 + \frac{12h}{w}}} \quad (4)$$

Finally, the effective dimension along the longest side is

$$L_{\text{eff}} = L + 2\Delta L \quad (5)$$

Here, length L is given as

$$L = \frac{1}{2f_r \sqrt{\epsilon_{\text{reff}} \sqrt{\epsilon_o \mu_o}}} - 2\Delta L \quad (6)$$

3 Design Methodology

For designing an antenna array, it is necessary to design a single patch antenna element. To find length of patch at 28 GHz use Eq. (6) which is equal to 3.152 mm, Using RT5880 LZ which is having 0.762 mm thickness and 1.96 permittivity. Width of the patch is 4.403 mm. These computed dimensions are listed in Table 1.

The return loss graph presented in Fig. 2 for the proposed design expressed excellent radiation characteristics. The resonant characteristics as read from the Fig. 2 plot clearly specify that the antenna has good response from 27.5 to 29.3 GHz. For the center frequency, the radiation pattern plot has been simulated and presented in Fig. 3 which shows patch antenna features. The single antenna design, simulation and analysis has been accomplished with the geometry, dimensions, return loss and radiation patterns plots. The characteristics of the single element patch antenna are evident from the plots presented from Fig. 1 through Fig. 3.

For improving the gain and impedance bandwidth two patch antenna element array is designed. Figure 4 shows the two element antenna array. The geometry of the array has to be taken into consideration after the properly defining the feed system. The feed systems considered in the present design is given in Fig. 4. Further, the dimensions of the antenna are given in Table 2. The antenna array with two elements has been designed and simulated on the advanced EM tool and the analyses using the simulated reports generated. The simulated reports include the S11 plot and radiation pattern plot.

Table 1 Proposed single element antenna dimensions

Parameters	Values (mm)
L	3.153
l	2.108
x_0	2.050
W	4.403
W_T	0.764
W_{50}	2.520

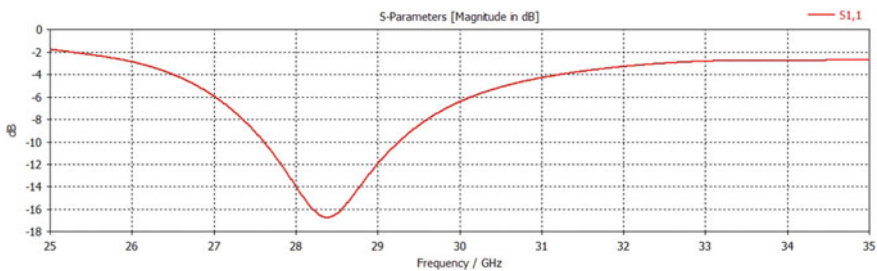


Fig. 2 Frequency response of S11

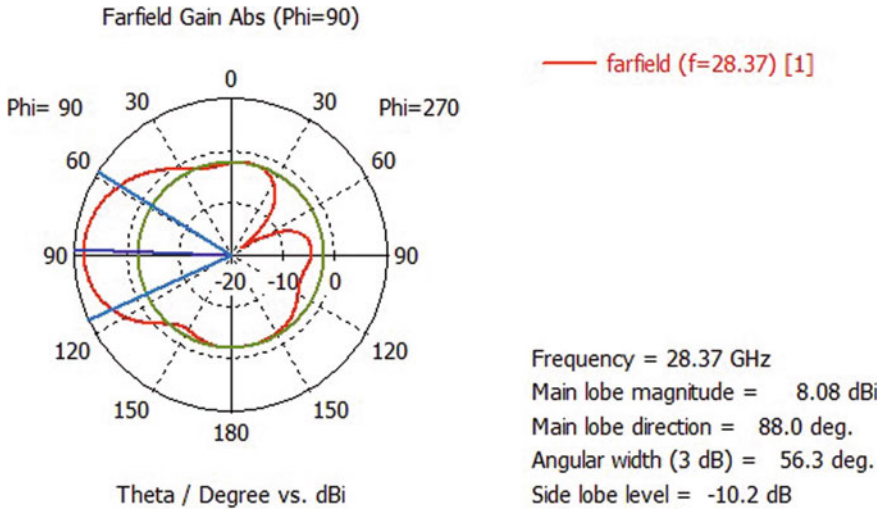


Fig. 3 Gain distribution

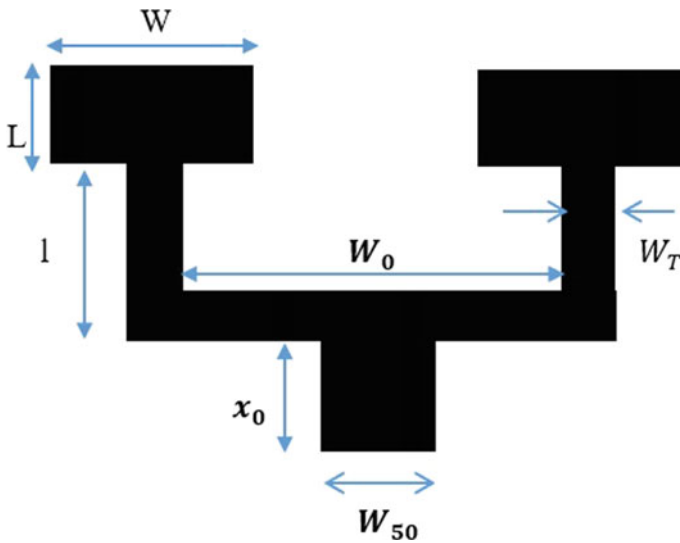


Fig. 4 Proposed two element configuration

The overall resonant features are evident from the S11 plot presented in Fig. 5 for the designed geometry of array.

The array geometry provided another resonant band which is evident from the return loss plot. Further, the gain characteristics are studied from the radiation pattern plot given in Fig. 6. The considerable increase in the gain is due to the fact that the

Table 2 Array configuration

Parameters	Values (mm)
L	3.153
l	2.108
x_0	2.050
W	4.403
W_T	0.764
W_{50}	2.520
W_0	13.522

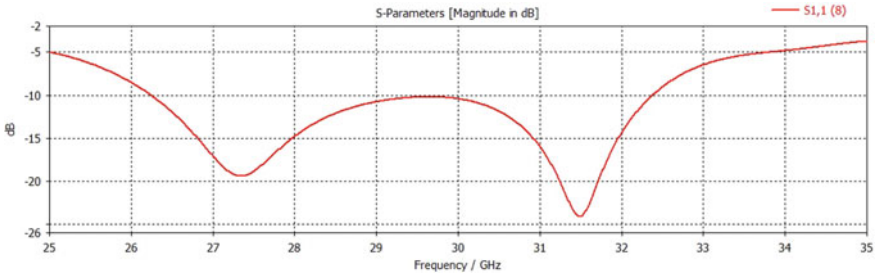


Fig. 5 S11 plot for the array

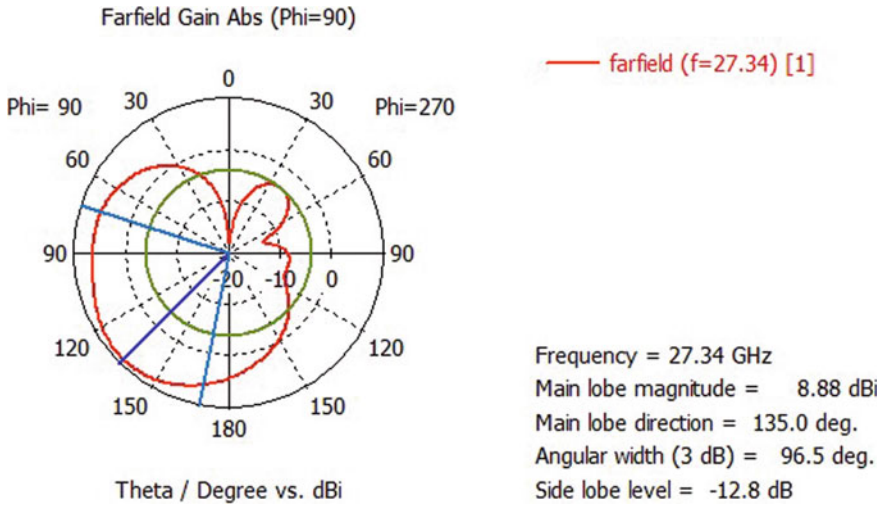


Fig. 6 Gain plot for the proposed array

array has features to enhance the gain of the antenna with multiple elements contained in it.

4 Conclusion

Initially, the single element of the patch antenna is designed for the center operating frequency of 28 GHz. It typically reported very narrow band and poor directivity and gain. The proposed antenna reported an operating range of 28.3–28.5 GHz. The corresponding bandwidth computed to be 8.2% with a gain of 8.08 dB. Following this, the array configuration of the proposed antenna reported an enhanced gain and bandwidth characteristics of by 28.86%. Can be concluded that it is the obvious advantage of array configuration.

References

1. Terlapu SK, Chowdary PSR, Jaya C, Chakravarthy VS, Satpathy SC (2018) On the design of fractal UWB wide-slot antenna with notch band characteristics. In: *Microelectronics, electromagnetics and telecommunications*. Springer, Singapore, pp 907–912
2. Balanis CA (2005) *Antenna theory analysis and design*. Wiley & Sons Ltd, New Jersey
3. Anguera J, Andújar A, Jayasinghe J, Chakravarthy VV, Chowdary PS, Pijoan JL, Ali T, Cattani C (2020) Fractal antennas: an historical perspective. *Fractal Fractional* 4(1):3
4. Ershadi S, Keshtkar A, Ershadi S, Abdelrahman AH, Yu X, Xin X (2016) Wideband subarray design for 5G an antenna arrays. In: *URSI Asia-Pacific radio science conference (URSI AP-RASC)*. Seoul, pp 185–187
5. Pozar DM (1989) On the design of low sidelobe microstrip arrays. In: *Digest on antennas and propagation society international symposium*, vol 2. San Jose, CA, USA, pp 905–908
6. Ali MMM, Haraz O, Alshebeili S, Sebak AR (2016) Broadband printed slot antenna for the fifth generation (5G) mobile and wireless communications. In: *17th International symposium on antenna technology and applied electromagnetics (ANTEM)*. Montreal, QC, pp 1–2
7. Parchin NO, Shen M, Pedersen GF (2016) End-fire phased array 5G antenna design using leaf-shaped bow-tie elements for 28/38 GHz MIMO applications. In: *IEEE international conference on ubiquitous wireless broadband (ICUWB)*. Nanjing, pp 1–4
8. Hong W, Baek KH, Lee Y, Kim Y, Ko ST (2014) Study and prototyping of practically large-scale mm wave antenna systems for 5G cellular devices. *IEEE Commun Mag* 52(9):63–69
9. Rahman SU, Khan MI, Akhtar N, Murad F (2016) Planar dipole antenna for tri-band PCS and WLAN communications. In: *Progress in electromagnetic research symposium (PIERS)*. Shanghai, China, Aug 8–11 2016
10. Chakravarthy VS, Rao PM (2015) Amplitude-only null positioning in circular arrays using genetic algorithm. In: *2015 IEEE international conference on electrical, computer and communication technologies (ICECCT)*. IEEE, Mar 2015, pp 1–5
11. Chakravarthy VVSS, Chowdary PSR, Anguera J, Mokara D, Satapathy SC (2021) Pattern recovery in linear arrays using grasshopper optimization algorithm. In: *Microelectronics, electromagnetics and telecommunications*. Springer, Singapore, pp 745–755
12. Gupta AK, Patnaik AK, Suresh S, Chowdary PSR, Krishna MV (2021) DGS-based T-shaped patch antenna for 5G communication applications. In: *Microelectronics, electromagnetics and telecommunications*. Springer, Singapore, pp 11–19

Novel Technique for Identification of False Coconuts to Avoid Genetic Diseases Using Classifiers



K. Murali, K. Prasuna, and G. Aloy Anuja Mary

Abstract Identification of true coconuts is one of the critical tasks in the applications of Image Processing. There are several methods in identification but out of them classifiers play an important role in identification. In this paper, classifiers are used to identify the true coconuts based on template matching. Genetic diseases can be identified using surveyed classifiers. Fast PCA classifier is the best classifier in identifying false coconuts.

Keywords Identification · Classifiers · Thresholding

1 Introduction

Visualization of true coconuts is the main application in Image Processing. The largest number of coconut trees are in India. Several cameras, sensors and other devices are used for identification of true coconuts to distinguish from false. As the technology is growing, severe scarcity of man power is affecting.

Now a days the society is more aware of health in this regard the cool drinks are diluted with chemicals most of the people are preferring coconuts rather than other drinks. The delta region in east Godavari district of costal Andhra Pradesh, India called the konaseema region. Konaseema region has numerous coconut trees and paddy fields. Konaseema coconuts are exported to various places of India and price of coconuts is less as the production is more. Coconuts are known for their versatility ranging from food to cosmetics they form a regular part of the diet of many people in the tropics and sub tropics coconuts are distinct from other fruits for their endosperm

K. Murali (✉) · K. Prasuna
Department of ECE, Vijaya Engineering College, Vijayawada, India
e-mail: kalipindimurali@gmail.com

G. A. A. Mary
Department of ECE, Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, India
e-mail: draloyanujamary@veltech.edu.in

containing a large quantity of water and when immature may be harvested for the portable coconut water.

The coconut is considered as “the image of the tropics” and “the tree of paradise” in perspective of its situation as a key ranch yield of the tropics and furthermore it is flexible commitment to mankind. Relatively all aspects of the coconut tree is utilized either to produce salary or to meet the sustenance necessities of rustic groups. Coconut items give nourishment, haven and vitality to cultivate family units, and can be made into different commercial and modern items. At the point when deliberately utilized, it can build sustenance generation, enhance nourishment, make employment openings, upgrade value and help to safeguard nature. Not with standing being a sustenance trim, coconut is considered as a modern harvest. The coconut business is personally associated with the monetary and household life of the tenants of coconut-developing states. The coconut palm has been known to exist in many districts of the tropics from pre-noteworthy circumstances. It is presently viewed as that the coconut palm may have begun autonomously in the Pacific and furthermore the Indo-Atlantic maritime bowls. People may have achieved its spread to different districts of the world through boats, and nature through ocean streams [1–3].

2 Problem Statement

Now a days as the atmosphere is polluted, coconuts are also polluted the kernel of the coconut root is injected with a monocrotophos, a pesticide and a carthoxine also known as luphos insecticide which is used in vegetables, trees and so on to destroy the flies but this pesticides is used in the root of the coconut and digged in the soil. In general after 40 days any of the fruit should be used as the pesticide injected into it.

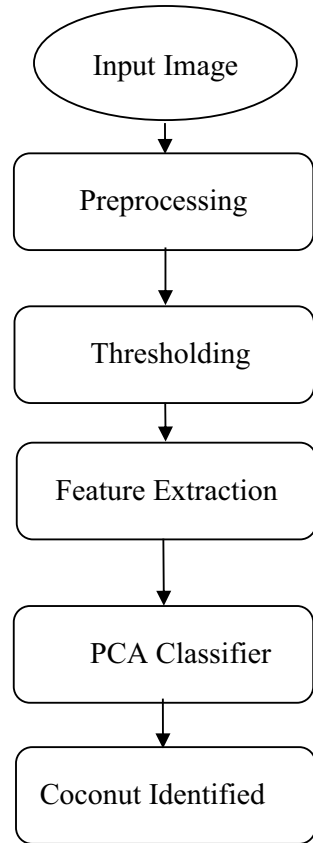
This pesticide affects liver, kidney, heart. It burns the heart. It burns the heart tissues in the body. It burns the heart tissues in the body. It also affects birds and animals also which is poisonous. Many genetic diseases are prevailed as the coconuts are used within 10 days which affects the health of the human beings. This can be overcome by our proposal.

3 System Model

Coconut Image with complex foundation may contain in excess of one question which may incorporate forefront objects, i.e., target developed coconut and foundation objects. So the foundation pictures must be dispensed with, for that the accompanying procedure needs to done [4]. Before that the camera ought to be utilized for getting the info pictures [5].

There has been a considerable measure of achievement in the improvement of successful parallel classifiers. Albeit numerous factual arrangement strategies do

Fig. 1 Proposed flow chat for coconut detection



have common multi-class augmentations, a few, for example, SVMs, do not. In this way, it is essential to know how to delineate multi-class issue into a set of less complex twofold arrangement issues. A standout among the most basic methodologies for multi-class from twofold is known as class binarization. A class binarization is a mapping of a multi-class issue onto a few two-class issues (isolate and-vanquish) and the resulting mix of their results to determine the multi-class forecast [6] (Fig. 1).

4 Classifiers

There are several classifiers out of which the best one can be chosen for application. Some of the classifiers are as follows:

(a) Ada Boost Classifier

AdaBoost calculation makes an arrangement of poor students by keeping up an accumulation of weights over preparing information and modifies them after each feeble learning cycle adaptively. The weights of the preparation tests which are misclassified by current feeble student will be expanded while the weights of the examples which are effectively characterized will be diminished [7].

(b) Modified AdaBoost Classifier

One of the principle thoughts of AdaBoost calculation is to keep up an appropriation or set of weights over the preparing set [8]. At first, all weights are introduced similarly, however on each round, the weights of inaccurately characterized cases are expanded with the goal that the powerless student is compelled to center around the hard cases in the exchanging set. The frail student's activity is to locate a frail theory $h: X \rightarrow \{ -1, 1 \}$ fitting for the appropriation [9].

AdaBoost is a standout among the most encouraging, quick meeting and simple to be executed machine learning calculation. It requires no earlier information about the powerless student and can be effectively joined with other technique to discover feeble speculation, for example, bolster vector machine. Two fundamental biometric acknowledgment applications: Face Detection and Facial Expression Recognition are given which related AdaBoost calculation for include extraction, highlight choice and classifier learning [10].

Any example order and acknowledgment issue can be viewed as machine learning and wise human PC association at last [11]. The objective of machine knowledge framework is to take in a characterization work from a given list of capabilities and a preparation set of positive and negative examples. The AdaBoost learning calculation is utilized to help the order execution out of some powerless students. This harsh list of capabilities must be chosen and refined before being submitted to classifier learning. Highlight choice is a streamlining procedure to decrease a vast arrangement of unique unpleasant highlights to a moderately littler component subset which containing just huge to enhance the characterization exactness quick and viably [12] (Fig. 2).

(c) Support Vector Machine

Support vector machine was produced by Vapnik from the hypothesis of Structural Risk Minimization. Be that as it may, the characterization execution of the essentially actualized is frequently a long way from the hypothetically anticipated. So as to enhance the characterization execution of the genuine SVM, a few specialists endeavor to utilize gathering strategies, for example, customary Bagging and AdaBoost. AdaBoost calculation are not generally anticipated that would enhance the execution of SVMs, and even they intensify the execution especially. This reality is SVM is essentially a steady and solid classifier [13, 14].

Fig. 2 Basic view of coconuts



(d) PCA Classifier

Foremost Component Analysis is a settled method for dimensionality decrease and multivariate examination. Cases of its numerous applications incorporate information pressure, picture handling, perception, exploratory information examination, design acknowledgment and time arrangement forecast. An entire exchange of PCA can be found in course readings [15, 16]. The ubiquity of PCA originates from three imperative properties. Initially, it is the ideal (as far as mean squared blunder) straight plan for packing an arrangement of high dimensional vectors into an arrangement of lower dimensional vectors and afterward reproducing the first set.

Second, [17] the model parameters can be registered straightforwardly from the information—for instance by diagonalizing the test covariance grid. Third, pressure and decompression are simple tasks to perform given the demonstrate parameters—they require just lattice duplication.

A multi-dimensional hyper-space is regularly hard to imagine. The fundamental goals of unsupervised learning techniques are to diminish dimensionality, scoring all perceptions in view of a composite list and bunching comparative perceptions together in view of multivariate characteristics. Abridging multivariate properties by a few factors that can be shown graphically with negligible loss of data is valuable in information revelation. Since it is difficult to imagine a multi-dimensional space, PCA is principally used to lessen the dimensionality of d multivariate traits into a few measurements [18, 19].

PCA abridges the variety in connected multivariate credits to an arrangement of non-associated parts, every one of which is a specific direct mix of the first factors. The extricated non-associated segments are called Principal Components (PC) and are assessed from the eigenvectors of the covariance framework of the first factors. Along these lines, the target of PCA is to accomplish niggardliness and lessen dimensionality by separating the most modest number segments that record for the vast majority of the variety in the first multivariate information and to compress the information with little loss of data [20, 21].

Fig. 3 Input image

PCA is used in this work as an exploratory multivariate examination strategy. Multivariate investigation is worried about informational indexes that have in excess of one reaction variable for each observational unit. The information sets can be condensed by information frameworks X with n lines and p sections, the lines speaking to the perceptions, and the sections the factors. The primary division in multivariate strategies is between those that accept a given structure, for instance, separating the cases into gatherings, and those that look to find the structure from the proof of the information network alone, likewise called information mining [22, 23]

(e) Fast PCA Classifier

One approach to process all the h orthonormal premise vectors is to utilize Gram-Schmidt technique. The most overwhelming/1 Note that the network reversal scales a s the solid shape of the framework measure. Correspondingly, all the rest of the $h - 1$ premise vectors (orthonormal to the already estimated premise vectors) will be estimated one by one out of a lessening request of predominance[24]. The already estimated $(p - 1)$ th premise vectors will be used for finding the p th premise vector. The calculation for p th premise vector will meet when the new and old qualities up point a similar way (Figs. 3, 4 and 5).

In PCA Classifier, 68% Disease is identified but by the use of fast PCA 75% is identified. This shows that Fast PCA works better in identifying the diseased coconut to a large extent.

5 Conclusion

There are so many methods in identifying coconuts but this paper presents a novel method, i.e., Fast PCA which proves better quality and true identification with best time consuming, also genetic diseases can be identified using classifiers (Figs. 6 and 7).

Fig. 4 Preprocessed image

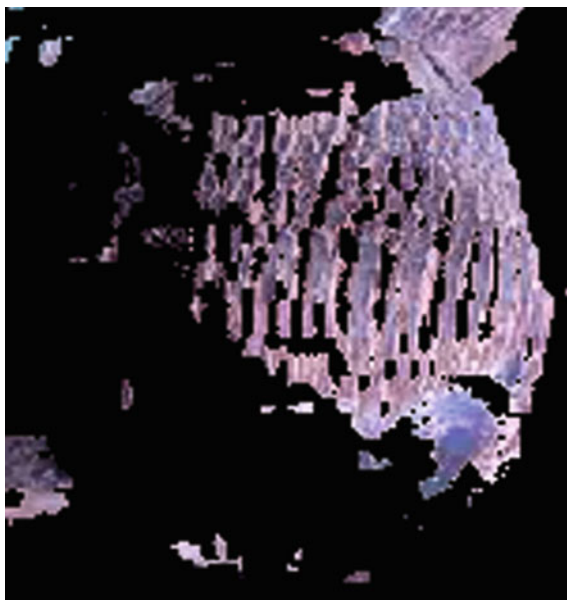
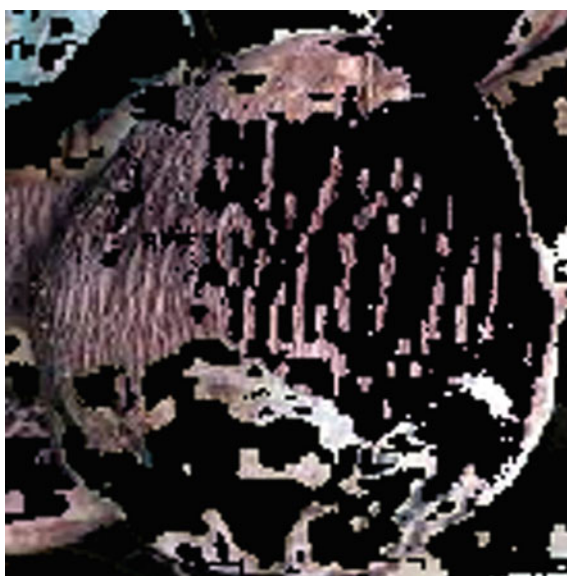


Fig. 5 Thresholded image



Type of Image	Contrast	Correlation	Energy	Homogeneity	Mean	Standard Deviation	Entropy	RMS	Variance	Smoothness	Kurtosis	Skewness
Non Diseased	0.581	0.9331	0.540	0.9525	38.31	70.6664	2.89	7.94	4590.595	0.9999	3.903	1.56
Diseased	0.392	0.9818	0.51	0.980	167.6	119.153	1.85	12.8	8390.44	0.99	1.47	-0.668

Fig. 6 Table showing features of extraction

Total no. of trainings 3409	Predicted: NO	Predicted: YES	Total no. of actual NO and actual YES values
Actual: NO	2458	2883	2507
Actual: YES	2528	2597	20256
Total no. of predicted NO and Predicted YES values	2711	69859	3409

Fig. 7 Table showing training and testing calculations

References

- Borovicka J (2013) Circle detection using hough transform. COMS30121—Image Process Comput Vis
- Hafizal Y, Haniza Y, Harun M, Mohd S, Rizon M, Juhari M, Shaharudin S (2007) Circular discontinuities detection in welded joints using Circular Hough Transform
- Hu R, Jia W, Ling H, Huang D (2012) Multiscale distance matrix for fast plant leaf recognition
- Murillo-Bracamontes EA, Martinez-Rosas ME, Miranda-Velasco MM (2012) Implementation of Hough transform for fruit image segmentation
- Murillo-Bracamontes EA, Martinez-Rosas ME, Miranda-Velasco MM, Martinez-Reyes HL, Martinez-Sandoval JR, Cervantes-de-Avila H(2012) Object Detection using Circular Hough Transform
- Hussin R, Juhari MR, Kang NW, Ismail RC, Kamarudin A (2012) Digital image processing techniques for object detection from complex background image. In: International conference on emerging engineering trends and science (ICEETS—2016) ISSN: 2348-8549, p 247
- Smereka M, Duleba I (2008) Circular object detection using a modified hough transform
- Parker JR (2011) Igorithms for image processing and computer vision, 2nd edn. Wiley Publishing, Inc., ISBN:978-1-118-02188-0
- Mohanty SP, Hughes DP, Salathé M (2016) Using deep learning for image-based plant disease detection
- Toontham J, Thongchaisuratkrul C (2011) Element14 beaglebone black hardware manual
- The comparison of object recognition and identificationby using image processing base on the neural network,the hough transform and the Harris Corner Detection
- Metev SM, Veiko VP (1998) Laser assisted microtechnology. In: Osgood RM Jr (ed), 2nd edn. Springer-Verlag, Berlin, Germany
- Schikora M, Neupane B, Madhogaria et al (2012) An image classification approach to analyze the suppression of plant immunity by the human pathogen Salmonella Typhimurium. BMC Bioinf 13(1):171
- Deshai N, Sekhar BVDS, Reddy PVGD, Chakravarthy VVSSS (2020) Processing real world datasets using big data hadoop tools. J Sci Ind Res (JSIR) 79(7):631–635
- Wegmuller M, von der Weid JP, Oberson P, Gisin N (2000) High resolution fiber distributed measurements with coherent OFDR. In: Proceeding ECOC'00, 2000, paper 11.3.4, p 109
- Cruz AC, Luvisi A, De Bellis L, Ampatzidis Y (2017) Visionbased plant disease detection system using transfer and deep learning. In: proceeding 2017 ASABE Annual International Meeting, Spokane, WA, USA
- Garcia-Ruiz F, Sankaran S, Maja JM, Lee WS, Rasmussen J, Ehsani R (2013) Comparison of two aerial imaging platforms for identification of huanglongbing-infected citrus trees. Comput Electron
- Garg R, Mittal B, Garg S (2011) Histogram equalization techniques for image enhancement. Int J Electron Commun Technol 107–111
- Haidekker M (2010) Advanced biomedical image analysis. Wiley Online Library
- Strange RN, Scott PR (2005) Plant disease: a threat to global food security. Phytopathol 43:83–116

21. Barbedo JGA, Koenigkan LV, Santos TT (2016) Identifying multiple plant diseases using digital image processing. *Biosyst Eng* 147:104–116
22. Ghaiwat SN, Arora P (2016) Cotton leaf disease detection by feature extraction. In: research advances in the integration of big data and smart computing, IGI Global, pp 89–104
23. Brahim M, Boukhalfa K, Moussaoui A (2017) Deep learning for tomato diseases: classification and symptoms visualization. *Appl Artif Intell* 31(4):299–315
24. Meunkaewjinda A, Kumsawat P, Attakitmongcol K, Srikaew A (2008) Grape leaf disease detection from color imagery using hybrid intelligent system. In: IEEE 5th International conference on electrical engineering/electronics, computer, telecommunications and information technology ECTI-CON, Krabi, pp 513–516

Privacy Preserving Datamining Techniques with Data Security in Data Transformation



Bonagiri Jyothi and V. Naga Lakshmi

Abstract Data mining is the process of pattern recovery in multiple database fields. Big data is the great volume of data that is being processed in the environment of data mining. It is therefore impossible to use hand-held database management tools or typical data processing programme to collect data sets, so that data mining techniques have been deployed. An effective data transformation is a vital prerequisite for facilitating an efficient process for discovering information on a wider scale. I would want to mention that in present PPDM research, certain fundamental problems are not addressed. First of all, Privacy Preserving Data Mining (PPDM) does not have a standard terminology. Second, for the centralised database, most algorithms are developed. However, data are commonly stored in several sites in today's global digital world. Third, many algorithms are focused on safeguarding the privacy of personal information, but do not focus on data mining results. There is no single approach to obtain data and to hide limitations. Fourth, each algorithm is specialised on data mining tasks primarily. No single strategy can work for any type of data clustering algorithm. Part of data privacy also is a crucial role in transforming data after data storage. These can be used as a guide to future PPDM research. Present research explores the privacy of data mining with various ways to approach the scope of new development approach.

Keywords Data mining · PPDM · Techniques · Algorithms · Review

1 Introduction

Deep learning is a machine learning branch based on many methods that strive to represent abstract, high-level data in visual processing layers with structural

B. Jyothi (✉) · V. N. Lakshmi

Department of Computer Science, Gitam (Deemed to be University), Visakhapatnam 530045, India

e-mail: jyothi.chekka@gmail.com

elements. Li et al. [1]. Deep learning belongs to a smaller collection of data representation approaches. An observation such as an intensity vector per pixel, can be represented in a more abstract fashion as a set of edges, regions of a certain shape, etc. Some of the techniques help to learn the tasks. (e.g. recognition of the face or face) Glauner et al. [2] examples. The capacity to understand deeply is to replace hand-crafting by effective algorithms for unchecked or semi-monitored functional learning and structure. Xiong et al. [3]. Studies in this field aim to improve representations and develop models to learn from unorganised huge data. Some of these depictions are based on developments in neuroscience and freely rely on nervous system interpreters, such as neural coding which tries to discover a relationship between diverse stimuli and associated neuronal responses in the organ. Olshausen et al. [4]. A few architectures have been developed in areas such as computer vision, automatic speech accuracy, natural speech processing, audio recognition, and bioinformatics in which reducing results have been shown in a number of different tasks for the development of neural networks, deep neural networks, deep creed networks, and recurring neural networks. Deep learning was also regarded in particular as a logo or a marketing of neural networks. Gomes [5] deep learning may be characterised as a machine teaching class that uses multiple layers of non-linear processing devices for extraction and transformation of features. The output from the preceding layer is used as the input in every consecutive layer. The methods can be supervised or unsupervised and pattern analysis and classification are covered (supervised). They are based on the (unsupervised) learning of several levels of data characteristics or representation. Testolin et al. [6] higher-level characteristics are derived in order to construct a hierarchical representation from lower levels. Such data representation belongs in the wider field of machine learning. Learn several levels of depictions corresponding to various abstract levels; levels constitute a hierarchy of notions. With the rapid evolution of data base, networking, and computer technology, a huge number of single data may be digitally merged and analysed, hence increasing the usage of data mining techniques for trends and patterns. This has raised global concerns about maintaining individuals' privacy. Privacy protected data mining (PPDM) refers to the field of data mining which aims to protect sensible data from uninvited or unwanted divulgence Swati et al [7]. A genetic algorithm is a natural system-based search technology. It is employed in the calculation as a classifier and is also utilised to optimise the findings. Most pattern recognition applications of Genetic Algorithm improve some classification process parameters. Gokulnath et al. [8]. Genetic algorithms have been utilised in order to determine optimal weighting for categorization. The classificatory K-nearest neighbour algorithm (KNN) is used to determine the function of fitness. First, the main component analytics (PCA) is a standard extract approach. Saritha and Sajimon [9] classification combinations are another area used for optimising genetic algorithms. It is also utilised in case-based categorization when picking the prototypes. Kiran et al. [10] of the three above mentioned data mining approaches, intrusion detection is extensively utilised because of the following advantages over other techniques:

1. No labelled training data set is necessary.

2. Training data shall not be classified manually.
3. No need for the system to be able to detect any new forms of intrusions.

1.1 Problem of the Statement

PPDM is a new era of research in data mining, where data mining algorithms are analysed for possible infringement in privacy. PPDM research usually takes one of the three philosophical approaches: (1) data hiding, in which sensitive raw data like identifiers, name, addresses, etc. PPDM is a fast-growing research area. Given the number of different algorithms has been developed over the past years, there is an emerging need of synthesising literature to understand the nature of problems, identify potential research issues, standardise new research area, and evaluate the relative performance of different approaches.

1.2 K-Means Clustering

K-means is a hard-partitioned method commonly utilised because of the simplicity and the fastness of the technique. As the metric of similarity, he employs Euclidean distance. Hard clustering means an item in a data collection is only one cluster at a time. It is an analytical clustering algorithm that organises objects into K-disjoint clusters based on their characteristics so that the items in the same class have similar qualities and those that are in separate clusters have distinct qualities (Figs. 1 and 2).

2 Survey About Previous Research Contribution

Sharmila et al. [11] clustering for Data Privacy Preservation Data Mining has been developed. They presented a distinctive breakdown of sports value Solved singular value decomposition (SSVD). It is superior to the current singular value decomposition (SVD) system concentrates on a variety of data mining techniques based on cryptography. It is used for smaller databases in particular. By applying cryptographic methods this research achieved great safety. Vijayarani et al. [12] Effective Hybrid C-Tree methodology for the safeguarding of sensitive data in data mining protection have been demonstrated. For the encryption process they have used special characters and ASCII codes. It is really helpful to protect data sets of a medical type. Venkataramana [13] presented a data mining technology for the safeguarding of sensitive data type data set in privacy. K-Anonymity techniques are employed to safeguard individual personal data for e-santé records and to produce the best outcomes in terms of accuracy. Kumar et al. [14] random response and geometric data disturbance approach were shown. Only numerical data sets can protect this

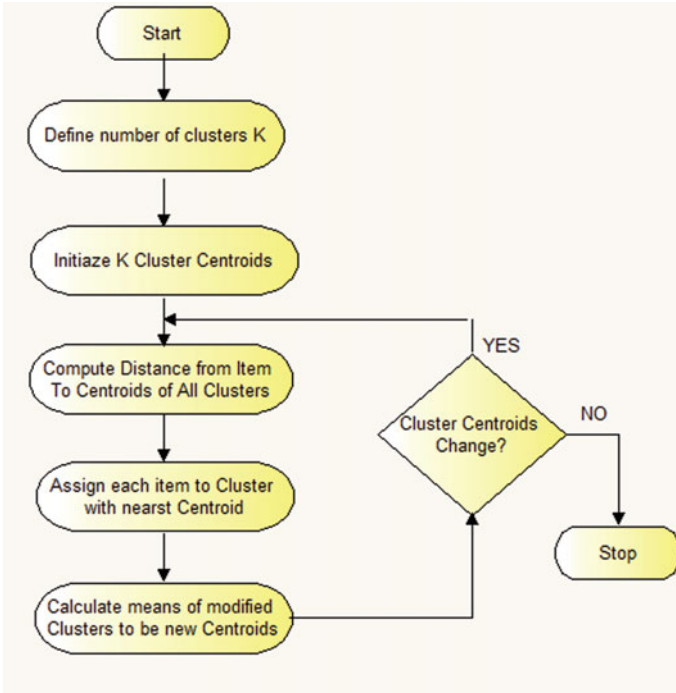


Fig. 1 Flow chart based on K-means clustering

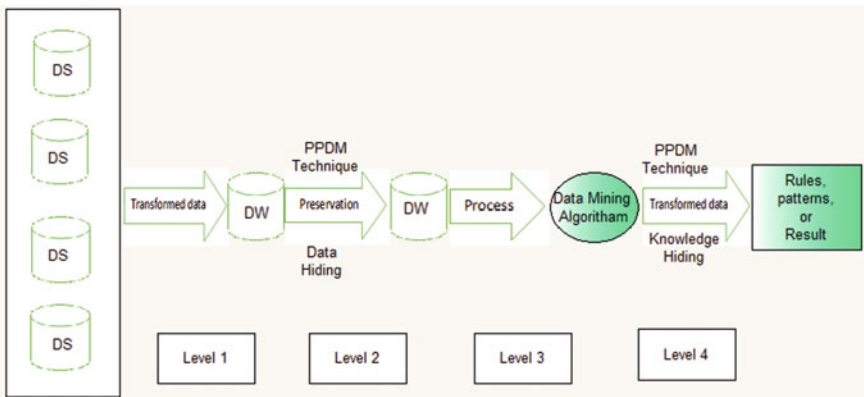


Fig. 2 Flow chart for data system implementation

strategy. Better protection of privacy than present technology. Nethravathi et al. [15] have projected random response approach geometric data disruption. This paper focuses on the numerical dataset solely. For categorical data sets, it is not applicable. Good accuracy results are maintained compared to previous strategies for data perturbation. Putri et al. [16] have defined various techniques and challenge problems linked to data mining privacy. The writers in this research explored the taxonomy of different data mining technologies for the protection of privacy and also numerous limitations of existing information mining methods for the protection of privacy. Yadav et al. [17] a new classification strategy has been demonstrated to assess privacy conservation of data mining utilising data interference approaches. Two strategies are utilised in the following work, namely, K-Anonymization and Data Perturbation. The authors kept their data utilities and data privacy stable. Fu et al. [18] presented an effective strategy for multiple disturbance based on the multiple value. They used K-means Clusters to gain more precision, recall, precision, and CMM calculations. Patil [19] a new approach for classifying data streams for data mining protection has been defined. Two important data mining phases, such as pre-processing and data stream mining, were included. They introduced a low information loss methodology of Hoeffding. Vijayarani et al. [12] proposed a technique of data transformation utilising the Normalisation for data correctness attained and the performance of the data mining algorithms improved. Zope et al. [20] defined a strategy based on maximum normalisation for data set privacy preservation of sensitive attributes. Using a minimum maximum normalisation, original dataset values are changed till the data mining begins. The experimental have shown that both the accuracy and the privacy of the suggested approach is retained. Acharjya [21] the concept for the preservation of sensory properties by clustering method in data set has been shown. The proposed method has managed to safeguard sensitive and vital information in the dataset, with good data mining results with minimal loss of information. Saraireh [22] the concept of geometric data interference has been demonstrated by means of k-mean clustering algorithms on modified and randomised data. To verify the correctness and produce high accuracy outcomes, the proposed method is applied. The experimental findings demonstrated that the original data without loss of information would be reconstructed by the proposed method.

2.1 Objectives PPDM Data Security Data Mining

- This size shall be determined to preserve anonymity in the classification of raw data using condensation methodology.
- Implementation of the hybrid technology that comprises hiding data and hiding knowledge.
- Implementing randomisation for a random approach to data security rotation.

3 Data Processing and Transformation

This strategy combines uncontrolled and controlled learning methods: first of all, generating a notion and then explaining the notion. The approach to explained data mining. This method comprises of a two-stage approach and uses two tables of data. A pattern is learned with one table. The other table, which consists of a profile of explanation for an interesting pattern, is used to look for pattern explanations (Fig. 3).

The model is then used to identify the remaining vast quantities of training data. The authors employed three widely known algorithms, for example, IB3, DROP3, and Genetic. Three prominent classification techniques are utilised, on the other hand, to generate training models for comparison: the CART decision tree and the K-nearest neighbour (K-NN) and support vector machines (SVM).

3.1 Data Transformation

The data are transformed or aggregated into mining forms in the transformation of data. The following can be the subject of data transformation: The data where low or “primitive” (rough) data is replaced in the use of concept Hierarchies through higher-level concepts. For example, the city and nation can generalise category properties, such as street, to higher notions. In the same way, values can be translated into higher-level concepts for numerical qualities such as age, young, middle-aged, and elderly. If the classification mining neural network back propagation algorithm is used, standardising the input values for each measured attribute in the training tuples will assist speed up the learning phase.

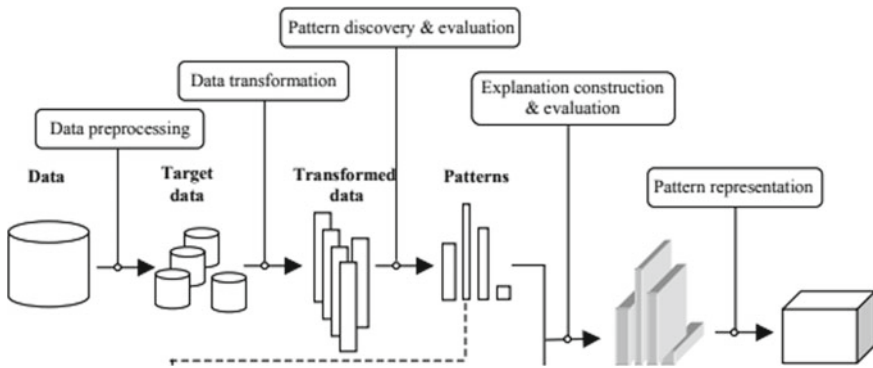


Fig. 3 Schematic diagram of data processing and transformation

3.2 Data Reduction

Data reduction techniques can be employed in order to obtain a significantly smaller, whilst closely maintaining integrity of the original data, reduced display of the data set. That is, the smaller data set should be more efficient and the analytical results should be achieved stated by Akhil [23].

3.3 Discretization and Concept Hierarchy Generation

When raw attribute data values are replaced with ranges or higher concept. Data discretisation is a form of reducing numbers, which is highly important for automatic concept hierarchy development.

3.4 Transformation Flow Chart

DFD shows what type of system input is needed and what form of system output is generated. What is the input for every module and from which data is kept and for who is the input. The DFD shows nothing about the operative sequence, the flow chart has been employed for this purpose (Fig. 4).

The users would be interested in abstract data that are not adequately known to them, yet they would like to understand them. Interactive approaches are therefore especially important to explore, analyse, and portray data or information visualisation concluded by Saidulu [24]. The challenge in information visualisation is to give the user visually the information that the user needs, so as to enable interaction mechanisms that allow visualisation to be efficiently and readily manipulated.

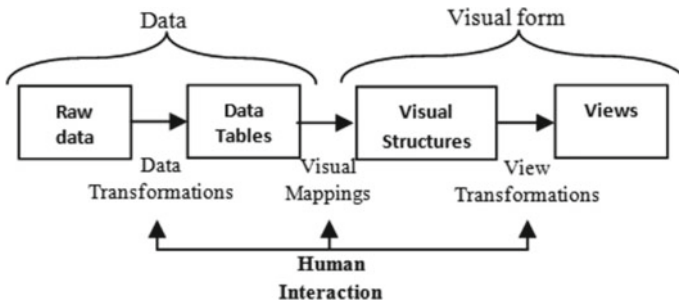


Fig. 4 Interactive mechanism

4 Algorithm Approach

To four times existing theories and practises of data analysis that protect privacy. First of all, to conduct a critical examination of diverse privacy preserving strategies and, in particular, a comprehensive study on state-of-the-art privacy preserving procedures for large-scale data analysis. Secondly, present a new 4-D framework for the systematic evaluation and successful design of the future generation of Big Data Analytics data protection approaches. Sivaram [25] express to identify the possibilities and challenges of using Big Data analysis in corporate environments that respect privacy also makes five proposals in order to guide empirical scientists and professionals interested in governing new privacy preserving big data analysis activities. Deshai et al. [26] replacing a value with a value that was less specific but semantically consistent, means blocking the values. K-anonymity is used to represent the method of anonymisation. The anonymization approach ensures that data are true after transformation, but that there is a certain loss of information.

4.1 Transformation Algorithm and Methodology

- To clearly identify technical strategies to achieve the business goals, it is necessary first to transfer the business objectives to a technological assignment.
- The relevant influencing characteristics (e.g. charge, condition) of the objective variables are necessary to derive methods. The parameters to be measured first need to be defined. The greater the complexity of system interactions, the more crucial becomes a systems approach. Here can be helpful methods such diagrams from Ishikawa, Pareto or cause-effect charts.
- The development of an appropriate measuring and data collecting technology requires a connection to the target DM algorithms. Technical performance criteria that depend not insignificantly on the data quality needed by the DM algorithm need to be known to be used to select measured methods and associated sensors. This is also true for the data transfer path.
- The DM project must consider the running production circumstances that should not have been disrupted by the DM project. The engineers' approach frequently takes this on board with evidence of concepts or test beds. These are used to design an initial solution outside of the production process. Following that, the implementation takes place in the production systems.
- The technical execution during deployment is an additional task. The objective of this large work is to transfer the functional and evaluated DM concept into the manufacturing application. This results in the following tasks
- First, you analyse the precise requirements of the DM concept for production. Ask how the integration of data gathering and transmission into the company network is additional.

- Develop a strong production system for acquiring and transferring data. Take the experience gathered through proof of conception studies into consideration.
- Implement permanent solution in the manufacturing systems. This entails integrating the technical part into the manufacturing system and integrating the software components into the IT environment of the company.

4.2 Data Security

Safety of information a huge amount of data is linked, examined, and dug for essential cases in big data analysis. Omana [27] describes Data security has therefore become an important problem for analysis of information. By using authentication, permission, and encryption technologies, big data safety may be improved. The extent of the network, the variety of gadgets, permanent safety control and the lack of a breaking framework are numerous security measures that big data apps encounter by Karthikeyan et al. [28]. Data security has been considered the safety challenge created by big data. In this context, the design of a multi-level security strategy and counteractive action framework must be taken into account.

4.3 Distributed Method-Based PPDM

Ying-hua et al. [29] Distributed Privacy Preserving Data Mining (DPPDM) was surveyed according to the various underlying technologies. There are three groups of available techniques such as (1) secure multiparty computation, (2) disturbance, and (3) restricted query. Experimental findings showed the usefulness of the system in detecting malfunctioning nodes and in improving the average network throughput. Furthermore, Mishra et al. [30] recognised the privacy dangers associated with cloud data mining and submitted a distributed framework for removing such hazards. The technique proposed included classification, disintegration, and distribution. This prevented data mining by keeping the data protection level, dividing the data into pieces and placing it into the appropriate cloud providers (Table 1).

Such anonymisation shall not only fulfil the underlying privacy criteria, it shall also protect the data's usefulness. K-anonymity is undoubtedly an efficient approach of data mining protection. However, a number of the data processed using this method often fail to resolve certain threats and are sensitive to the use of the Internet. Therefore, the future data protection privacy of K-anonymity based on data mining needs a new data infrastructure to accommodate the integration of current data features. Natarajasivan et al. [31] that would surely meet the requirements of various types of customers and communities. The current search algorithms are able to increase the retrieval process, but because of the linear increases in the response time by the amount of sought data, they do not scale up to enormous amounts of data.

Table 1 Description of PPDM methods

PPDM methods	Description
Data distribution	May contain vertically or horizontally partitioned data
Data distortion	Contain perturbation, blocking, aggregation or merging, swapping, and sampling
Data mining algorithms	Encloses classification mining, association rule mining, clustering, and Bayesian networks, etc
Data or rules hidden	Denotes to hide main data or rules of innovative data
K-anonymity	Achieve the anonymization
Randomisation	A complex and valuable strategy for concealing the individual PPDM data
Privacy protection	It should carefully adapt the data to select the highest data utility, protects the privacy

5 Conclusions and Future Objective

A new view is offered through explanatory data mining. It relates closely to scientific research and database mining using advantages. The concept of generalizable mining can substantially affect the understanding of data mining and the efficient use of data mining results. Total IT industry professionals, engineers working in data mining and in deep learning now have a day to come. Many people are offered different system models, Big Data techniques. Data Mining and Deep Learning Techniques in this study review. The approach presented takes into consideration the complexity of the various observation textual data that the user shares. By using any basic transformation approach to address data volumes and unstructured data form. Data mining algorithms focus on the mathematical nature of the information, rather than its private nature. Traditional ways to data mining and profound learning now a day. DM is a technique through which a big amount of information is discovered and analysed on a regular or semi-automatic basis. It is used to investigate and analyse massive amounts of data to find patterns for large data. All commercial transactions have been collected in a large database in recent years by all companies and marketers. It needs the working of new, generally called Large Data methods, new technology and communication.

References

1. Li D, Yu D (2014) Deep learning: methods and applications. Found Trends Signal Process, Now Publishers
2. Glauner PO (2015) Deep convolutional neural networks for smile recognition. arXiv preprint
3. Xiong M, Chen J, Wang Z, Liang C, Zheng Q, Han Z et al (2015) Deep feature representation via multiple stack auto-encoders. In: Advances in multimedia information processing—PCM 2015, Springer, pp 275–284
4. Olshausen BA (1996) Emergence of simple-cell receptive field properties by learning a sparse code for natural images. *Nature* 381:607–609
5. Gomes L (2014) Machine-learning maestro michael jordan on the delusions of big data and other huge engineering efforts. *IEEE Spectr* 20
6. Testolin A, Stoianov I, De Filippo De Grazia M, Zorzi M (2013) Deep unsupervised learning on a desktop PC: a primer for cognitive scientists. *Front Psychol* 4:10.3389
7. Swati K, Kumar S A comparative study of various data transformation techniques in data mining. *Int J Sci Eng Technol* 4(3):146–148, ISSN: 2277-1581
8. Gokulnath C, Priyan MK, Balan EV (2015) Preservation of privacy in data mining by using PCA based perturbation technique. In: 2015 International conference on smart technologies and management India, 6–8 May 2015, pp 202–206
9. Saritha K Sajimon Abraham big data challenges and issues: review on analytic techniques *Indian Journal of Computer Science and Engineering (IJCSE)*ISSN: 0976–5166 Vol. 8 No. 3 Jun-Jul 2017
10. Kiran A (2019) Data mining: random swapping based data perturbation technique for privacy preserving in data mining. *Int J Recent Technol Eng (IJRTE)* 8(1S4), ISSN: 2277-3878
11. Sharmila S, Vijayarani S (2017) Frequent item set mining and association rule generation using enhanced Apriori and enhanced Eclat algorithms. *Int J Innov Res Comput Commun Eng* 5(4)
12. Vijayarani S, Tamilarasi A (2010) Data transformation technique for protecting private information in privacy preserving data mining advanced computing. *An Int J (ACIJ)* 1(1)
13. Venkataramana S, Sekhar BVDS, Raju VS, Chakravarthy VVSSS, Srinivas G (2020) An experimental analysis of secure-energy trade-off using optimized routing protocol in modern-secure-WSN. *EAI Endorsed Trans Scalable Inform Syst* 7(26)
14. Kumar PK Novel framework for data transformation for yielding structured data in opinion mining. In: 2017 International conference on electrical, electronics, communication, computer and optimization techniques
15. Nethravathi NP, Rao PG CBTS: correlation based transformation strategy for privacy preserving data mining. In: *IEEE transactions on knowledge and data engineering*, vol 24, no 2, Feb 2012
16. Putri AW, Hira L (2016) Hybrid transformation in privacy-preserving data mining 978-1-5090-5671-2/16/©2016. *IEEE*
17. Yadav C, Wang S, Kumar M (2013) Algorithm and approaches to handle large Data-A Survey. *IJCSN Int J Comput Sci Netw* 2(3):2277–5420, ISSN (Online)
18. Fu Z A computational study of using genetic algorithms to develop intelligent decision trees 0-7803-6657-3/01/@ZOO O1. *IEEE*
19. Patil DV, Bichkar RS (2010) Multiple imputation of missing data with genetic algorithm based techniques. *IJCA Special Issue on Evolutionary Comput Optim Tech ECOT*
20. Zope AR, Vidhate A, Harale N (2013) Data mining approach in security information and event management. *Int J Future Comput Commun* 2(2)
21. Acharjya DP (2016) A survey on big data analytics: challenges, open research issues and tools. *(IJACSA) Int J Adv Comput Sci Appl* 7(2)
22. Saraireh S A secure data communication system using cryptography and steganography. *Int J Comput Netw Commun (IJCNC)* 5(3)
23. Akhil S, Uma K (2017) Survey on the challenges and issues on big data analytics. *Int J Mech Eng Technol (IJMET)* 8(12):138–149
24. Saidulu D (2017) Machine learning and statistical approaches for big data: issues, challenges and research directions. *Int J Appl Eng Res* 12(21):11691–11699, ISSN 0973-4562

25. Sivaram N, Ramar K (2010) Applicability of clustering and classification algorithms for recruitment data mining. *Int J Comput Appl* (0975–8887) 4(5)
26. Deshai N, Sekhar BVDS, Reddy PVGD, Chakravarthy VVSSS (2020) Processing real world datasets using big data Hadoop tools. *J Sci Ind Res (JSIR)* 79(7):631–635
27. Omana J, Monika S, Deepika B (2017) survey on efficiency of association rule mining techniques. *Int J Comput Sci Mobile Comput* 6(4):5–8
28. Karthikeyan T, Ravikumar N (2014) A survey on association rule mining. *Int J Adv Res Comput Commun Eng* 3(1)
29. Ying-hua L, Bing-ru Y, Dan-yang C, Nan M (2011) State-of-the-art in distributed privacy preserving data mining. In: *IEEE 3rd international conference communication software and networks*, pp 545–549
30. Mishra S, Mishra P (2014) A survey on association rule mining algorithms performance analysis. *Int J Eng Res Technol (IJERT)* 3(8), *IJERT/IJERT* ISSN: 2278-0181
31. Natarajasivan D, Govindarajan M (2016) Context aware user interface recommendation system. *Int J Innov Res Sci, Eng Technol* 5(5), *ISSN(Online):* 2319-8753

Rectangular Slotted Elliptically Placed Compact Antenna For Wide Band Applications at K and Ka Bands



A. V. Swathi, Akash Kumar Gupta, M. S. S. S. Srinivas,
B. S. S. V. Ramesh Babu, and P. Satish Rama Chowdary

Abstract The proposed work is on rectangular slotted antenna for wide band applications in K and Ka bands. The slots were arranged elliptically with edge feed. The design has achieved a bandwidth of 2 GHz resonating at K band with -22.5 dB reflection coefficient and 3.5 GHz bandwidth resonating at 26.5 and above at Ka band with -40 dB reflection coefficient. The proposed antenna is very light in weight and has very compact size which can be used for satellite applications. The resonant frequency of the proposed antenna finds applications in satellite uplinking, astronomical observations and radars. The antenna was simulated and fabricated, and the result provides good VSWR, impedance bandwidth, reflection coefficient and radiation pattern.

Keywords Edge feed · Rectangular slotted antenna · Elliptical · Compact antenna

1 Introduction

Wireless technology is one of the modern technologies that take a rapid growth in last few years. This fast growth of technology gave many challenges to researchers regarding the design of antenna. Various wireless devices have been manufactured which will inter-communicate with the other electronic gadgets in the name of networking. This networking when takes path in wireless technology antenna miniaturization comes into picture. The demand of compact antenna has been increased day by day in the field of electronic technology. The compact antennas were used

A. V. Swathi · A. K. Gupta · M. S. S. S. Srinivas (✉) · B. S. S. V. R. Babu ·
P. Satish Rama Chowdary
Department of ECE, Raghu Institute of Technology, Visakhapatnam, India
e-mail: srinumodali@gmail.com

B. S. S. V. R. Babu
e-mail: rameshbssv@ieee.org

P. Satish Rama Chowdary
e-mail: satishchowdary@ieee.org

for connectivity between gadgets such as Bluetooth, Zigbee, WLAN and WIMAX. This demand has been increased in satellite communication for signal uplinking, astronomical observations, RADAR communications and other various wireless applications which are at frequencies between 20 and 35 GHz.

The modern antenna design mostly gives regards to the multiband features in compact antenna system. These slotted antenna methods are investigated for various geometrical shapes with features of multiband. This research work focused on slotted antenna with dual and multiband features of antenna. The methodology based on the review of various literatures from slotted antenna was studied, and the compact antenna was proposed. Radar systems, satellite communication and astronomical observation all these areas of wireless communication need multiband antenna, and it is the key requirement behind all these inputs. For multi-mode radars and multi-object tracking radars, the study of astronomical elements needs multiband antenna. With all the above and from the literature review, it is understood that slotted antenna plays a vital role to have multiband antenna for applications at K and Ka bands.

The compact antennas in their primary stages are agreed to be as narrow band antennas with bandwidth less than 10%, and this parameter of the antenna limits the performance and application of the antenna. From various literature survey on using slots in antenna that have claimed to enhance bandwidth and reduce return loss, gain will be increased, and axial ratio and radiation pattern also improved. With the motivation from above features, multiband antenna at K and Ka has been proposed in this research with increased gain and improved bandwidth. On the other side, edge feed will reduce the spurious radiations from the antenna radiations.

Multiband antennas are the most vital components astronomical observations RADAR, and medical applications furthermore their wide frequency bandwidth, simple structure, ease of fabrication and its radiation patterns gave significance in its design. The electrical properties of these antennas are dependent on the number of slots element and also the ground plane. The antenna operates in the ultra-wideband covering the frequency ranging from 2 GHz to more than 40 GHz. The radiators of planar monopole antennas can be of any shape for broad operating bandwidth. The planar monopole circularly shaped antenna is known to work effectively in the ultra-wideband which makes it ideal for UWB applications.

2 Design of Antenna and Simulation

The geometry of the slotted antenna is shown in Fig. 1. It consists of a eight rectangular-shaped slots with 3×3 mm slot size with a radial gap of 2.5 mm arranged in an elliptical shape, the ground plane is 10×10 mm, antenna is printed on FR-4 substrate with relative permittivity $\epsilon_r = 4.4$ with substrate height $h = 1.6$ mm, and coaxial feed is used as antenna feed.

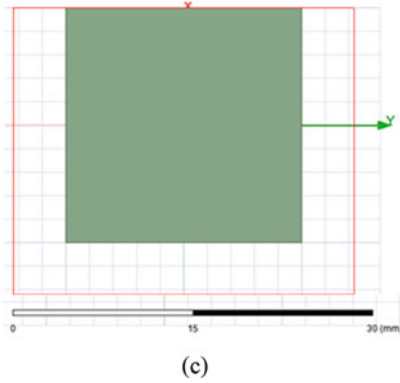
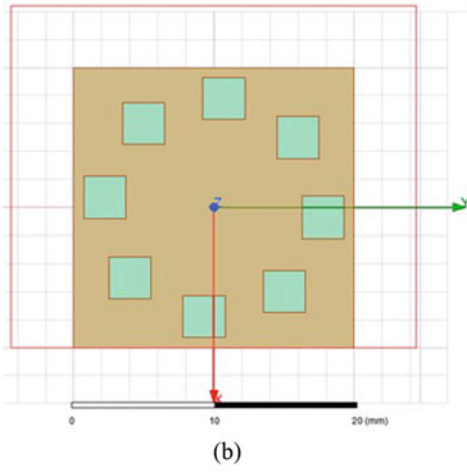
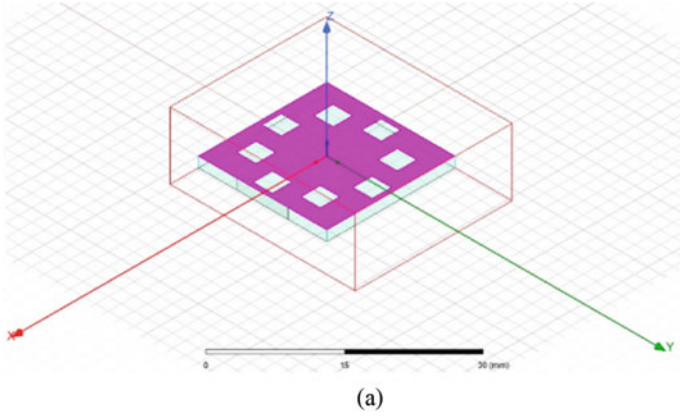


Fig. 1 a Slotted wide band antenna (ISO), b front view and c back view

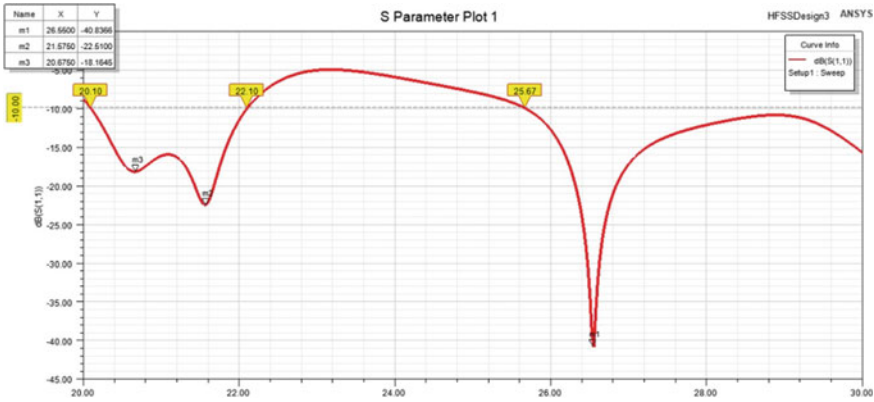


Fig. 2 Simulated reflection coefficients for the slotted antenna

Table 1 Design parameters

Design parameters	Dimensions In Mm
Ground plane length	10
Ground plane width	10
Slot size	3 × 3
Radial slot gap	2.5
Substrate height	1.6
Substrate FR4 ϵ	4.4

The performance of the antenna is investigated by carrying out a detailed analysis of the results. Figure 2 shows the return loss curve simulated by the antenna. As evident from the curve, it operates well in the K and Ka bands. The design parameters are tabulated (Table 1).

The simulated provided an excellent dual-band bandwidth of 2 GHz being antenna resonating at 21.5 GHz with -25 dB and another at 26.5 GHz with -41 dB as reflection coefficient, and the band is extending in K and Ka bands (Fig. 3).

The 2D simulated radiation pattern indicates a dumb-bell shape in the E-plane and almost omnidirectional radiation pattern in the H-plane at 20.5 GHz. The patterns are stable throughout the K and Ka bands. Also the radiation patterns are evident from the figure; at 26.5 frequencies, the E-plane possesses a dumb-bell-shaped pattern with normalized gain 9.4 and H-plane possesses an omnidirectional pattern.

Figure 4 shows the 3D polar plot characteristics of the proposed model at operating frequency bands. Finally, slotted antenna provides diversified patterns so as to attain improvement in reliability. Figure 5 displays the final antenna surface current densities at the edge feed of multi-slotted antenna at K and Ka frequency bands, i.e. 20.5 and 26.5 GHz. It is clearly evident from the figures that current coupled from patch slot 1 to patch slot 2 is providing excellent radiation in the E-plane. The normalized gain is considered, and the gain has achieved the required band of

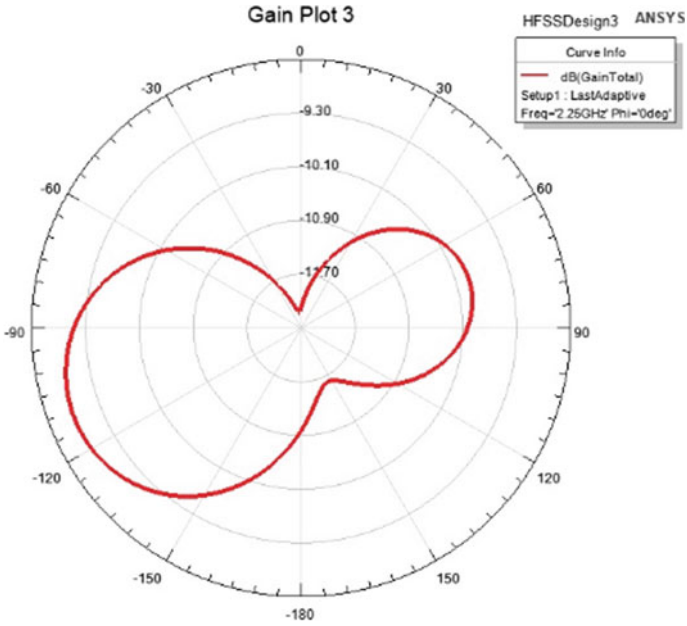


Fig. 3 Simulated 2D radiation patterns

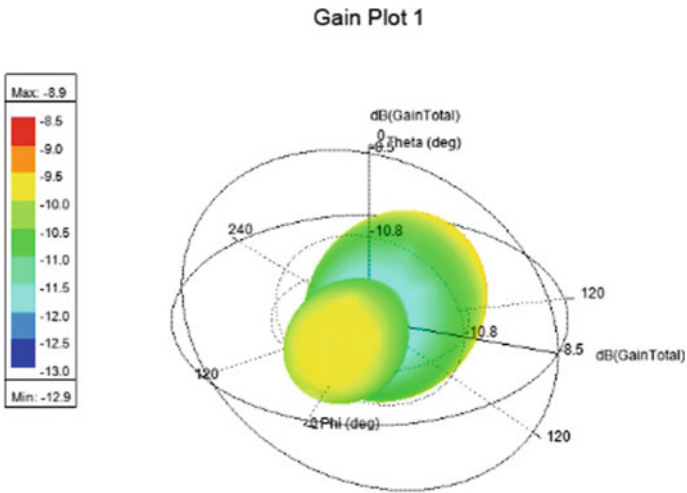


Fig. 4 Simulated 3D polar plots

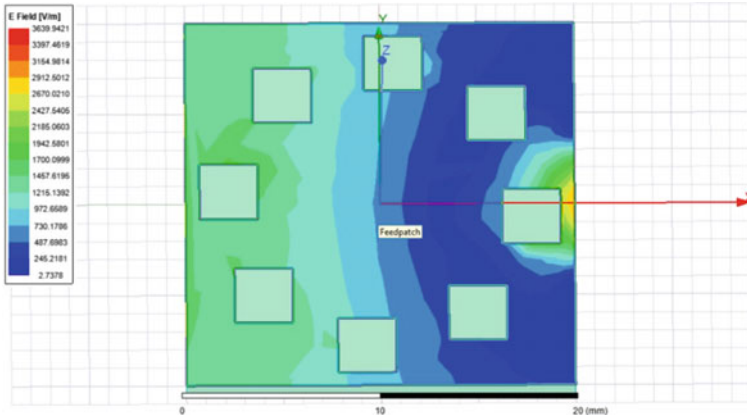


Fig. 5 E-field distribution of the antenna

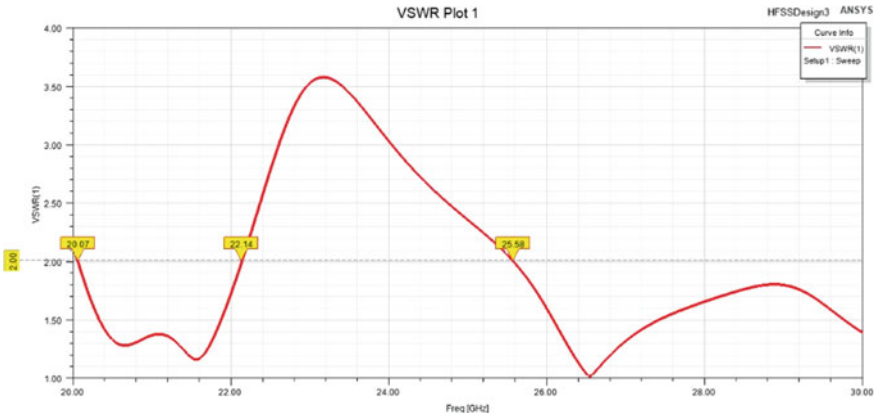


Fig. 6 Gain versus frequency plot

frequencies with very low reflection coefficient. Figure 6 shows the VSWR reading which is between 1 and 2 at the operating frequencies which is making the antenna more reliable and was above the limit at the stop bands.

3 Results and Discussion

The reflection co-efficient of the proposed antenna with simulation tool HFSS. It has been observed that the antenna is showing wide bandwidth of 2 GHz with characteristics from 20.10 to 22.10 GHz; the proposed antenna is also showing stop band

at the frequency from 22.10 to 26.5 which is covering other remaining communication bands up to 26.5 GHz and is extending. Figure 6 provides the VSWR curve that claims the VSWR between 1 and 2 at the resonating frequencies; also from the figure, we can observe that at the stop band, the VSWR raises above 2.

The current distributions of E-field and H-field shown in Fig. 7 provide current distributions at the feed in high and moderate at the patch. The fabricated patch is shown in Fig. 8.

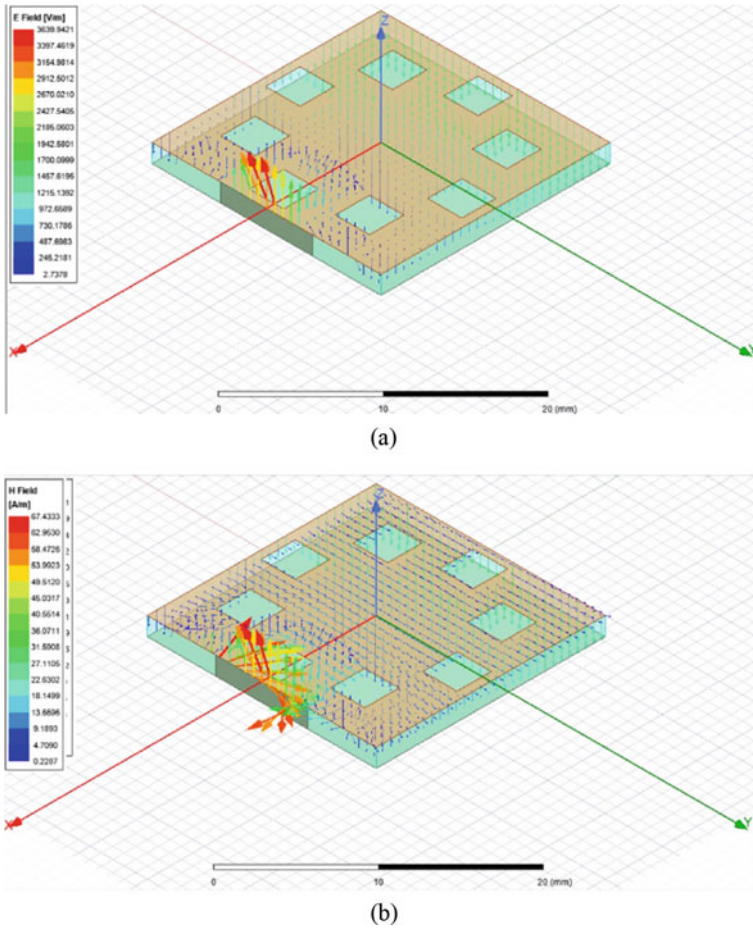


Fig. 7 Current distribution

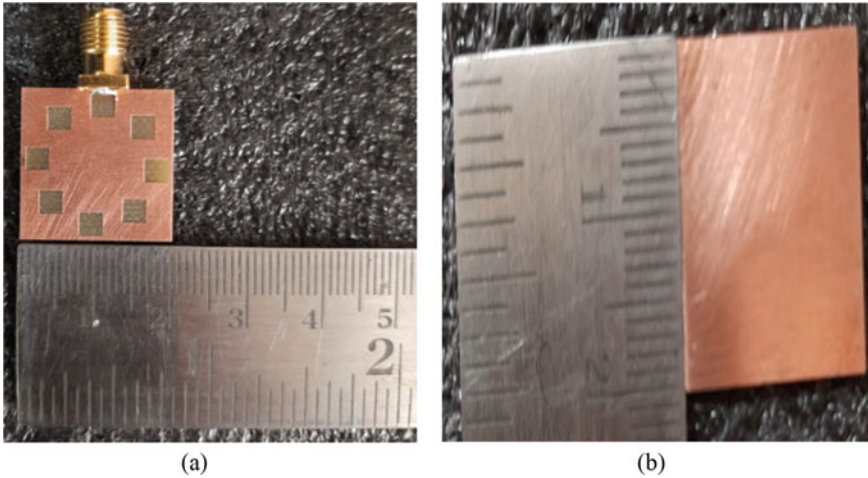


Fig. 8 Fabricated antenna

4 Conclusions

This paper discusses slotted antenna with edge feeding; the antenna resonates at 20.10 GHz and 26.5 GHz with 2 GHz bandwidth; at 26.5 GHz, the antenna shows wide bandwidth; the bandwidth extends towards 30 GHz. The antenna finds applications at these frequencies for astronomical observations, radars, satellite uplinking, etc., and the antenna also shows stop band between 22.10 and 26.5 GHz and provides good radiation pattern with VSWR between 1 and 2 at the resonating frequencies. By choosing various design structures such as slots arranged in circular, elliptical and hexagonal and also by changing the number of slots and the size of the slots, we can design antenna for several of the applications. The main advantage of the antenna is its lightweight, low profile and small size and can be incorporated in satellites, planes, and drones for intercommunication. Also by increasing the size of the antenna, a wide application at UWB, WiMAX, WLAN, Bluetooth, etc., can also be incorporated.

CAN Intrusion Detection Using Long Short-Term Memory (LSTM)



Srinivasa Rao Nandam, Adouthu Vamshi, and Inapanuri Sucharitha

Abstract Car hacking is becoming prevalent with new cyber techniques to hack any car by hacking its internal network controller. Most internal networks of a car are being controlled by a controller area network (CAN). The networks lack security systems to prevent cyber-attacks but intrusion can be detected using predictive analysis. We will use deep neural networks to detect the intrusion and will create a robust intrusion detection system which can be readily deployed. We specifically designed a DDoS attack detection system using LSTM. The network achieves 80% accuracy using only a few parameters.

Keywords Intrusion detection · Deep learning · Vehicular systems · CAN

1 Introduction

Recent trends in automotive industry have led to cars which have connectivity to World Wide Web and applications that use the internet for providing services to the driver [1]. Traditional mechanical controlled parts of a car like brakes, throttle, steering are now being controlled by electronic components [2]. These parts of the car are controlled by electronic control units (ECUs). To allow communication between devices inside the car, a networking devices like controller area network (CAN), local interconnected network (LIN) or a FlexRay [3] are used. To provide an economical, e client and easy communication, controller area network which is a message broadcast system is developed. CAN sends short relay message about the status of the vehicle to all the ECUs to maintain data consistency [4].

Because security adds another layer of complexity, CAN does not implement security features like encryption. There have been lot of security vulnerabilities

S. R. Nandam (✉) · A. Vamshi
Department of Computer Applications, NIT, Tiruchirappalli, India
e-mail: nandamsrinivasarao85@gmail.com

I. Sucharitha
Department of Information Technology, CBIT, Hyderabad, India

displayed by researchers for CAN [5]. They show that fabricated messages can be easily designed and injected into CAN to control or damage the vehicle. Different ways of injected fabricated messages are through wireless network in the vehicle; diagnostic port [6–8] shows various vulnerabilities that were discovered in vehicle systems.

Symmetric key cryptography has been used to increase the security of CAN protocol which is based on digital signatures [9, 10]. Using digital signatures can overload a CAN which is capped at 500kbps. Intrusion detection systems have been introduced to negate network traffic overhead, and it can be applied directly to existing systems. We specifically design an intrusion detection system which has been developed for detecting denial-of-service (DoS) attacks which uses a recurrent network to accurately detect DoS attack. The number of parameters of the network is very less compared to other convolution-based approaches [11].

The model uses a simple data processing technique, and we use the CAN id of arriving messages to detect the DoS attack which can be used by other systems to stop the communication in case of an attack. A sequence of previous messages is stored and passes with a current message as an input the model to predict the DoS attack.

2 Related Work

We will discuss previous work done from the perspective of data format and domain of the data.

2.1 CAN Intrusion Detection Models

CAN or other similar in-vehicle network is crucial to the working of a vehicle; any attack on the system can result in serious damage to both the vehicle and the driver. A message with a particular CAN ID sends messages to ECUs at specific rate. Miller and Valasek [12] have used the frequency of the specific CAN ID messages to detect the attacks. Entropy has been used to detect anomaly in CAN [13]. Entropy between ground truth reference and the actual network is compared to detect if an anomaly is present. Larson et al. [14] uses the specification of the protocol or ECU behaviour and based their predictions on them to detect intrusion. A timing analysis of occurrence of the CAN messages is used to develop a lightweight intrusion detection system [15]. The period at which the CAN messages are received is used a feature to separate normal message from an anomalous message. A clock-based intrusion detection system is developed and uses difference of frequencies between real clock and true clock for pro ling ECU behaviour [16]. Methods discussed until now have been based on specific conditions like periodicity of messages or other behaviour to detect intrusion. These methods may not always lead to better results which lead to the

development of deep learning models. Deep belief networks have been used for developing a classifier for detecting anomalous messages [17]. Generative adversarial networks are used to learn a generator to generate anomalous messages and also to detect anomalous messages [18]. Hierarchical temporal messages (HTM) are used to compute anomaly score to detect intrusion [19]. Hidden Markov model (HMM) has been used to detect normal messages in a vehicle [20].

2.2 Models Based on Nature of Data

Sequential data-based anomaly detection is an important research area. Chandola et al. [21] have proposed three different approaches to anomaly detection and uses a sequential data. Xing et al. [22] proposed a classification for sequence based detection methods. They can be either feature based methods which map the data to a feature vector or methods which measure the distance between test and reference sequence or models which are based on classification. Other system use system call data to detect intrusion. Hofmeyr et al. [23] use sequence calls of UNIX programs for developing intrusion detection system. System call traces have been analysed for detecting anomalous messages [24]. Data mining can also been used on system call data to detect intrusion [25, 26] uses agent based which analyse the system call, logs, network activity. Machine learning models for detecting anomaly have been used in android devices and use activity that occurs in a mobile [27], and also network intrusion has been devised [28]. Hurst parameter has been used to for a self-similarity-based intrusion detection [29]. Mobus traffic has been used to detect intrusion in SCADA systems. Network traffic has been converted to image and classified with a CNN [30].

3 In-Vehicle Network Overview

3.1 Controller Area Network (CAN)

CAN makes communication between ECUs possible by allowing them to communicate with each other; it is a message-based protocol. It has become popular in automotive industry and has been used widely. The ECUs are connected to the CAN with CAN low and CAN high wires. Figure 1 shows how the overview of logic of how a bit is signalled in CAN. When the transmitted bit is 0, then CAN low is zero volts and CAN high is five volts; in case of when bit is 1, then both CAN low high and low are 2.5 V. The messages are sent between ECUs, and their priority is as shown in Fig. 3.

Each message can be identified by a CAN ID. It contains almost 29 bits when extended and 11 bit normally. The message format for CAN has been shown in Fig. 2.

Fig. 1 Bit logic of a CAN

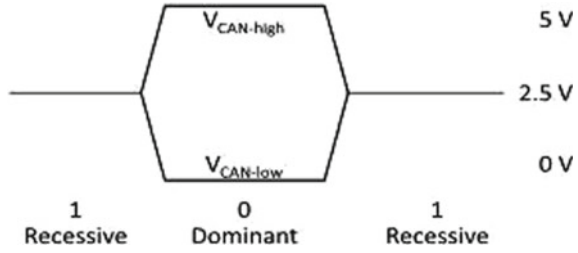


Fig. 2 Format of a CAN message



Fig. 3 Message arranged by priority in CAN

CAN has a specification defined for identifiers but the vehicle vendors customise it according to their needs. We apply our model on the sequential data from this CAN to detect intrusion.

3.2 Injection of Messages

CAN lacks most of the security features like authentication, encryption. Without authentication, we can stop nodes from connecting to CAN to modify or snoop message. One can analyse the network traffic by connecting to CAN and perform an injected message attack to either control or damage vehicle. Attackers have used various exploits to inject messages into a CAN [6]. These attacks are done either wirelessly or using a debug port. We introduce a model which can detect the incoming messages to CAN to identify whether DoS attack has been performed on the device. The intrusion detection system can be deployed as a node to the CAN to detect intrusion.

4 Model for Intrusion Detection

We develop an intrusion detection system based on recurrent neural networks. The CAN data is a sequence based data. We try to use the sequential nature of the data to perform our detection. The prediction is similar to time series prediction. In time series prediction, we classify the current time step based on values on the previous time steps. We consider in our network previous 50 time steps to make prediction on the current time step. Recurrent networks contain recurrent connection between nodes and share weights across the whole sequence to make prediction.

The hidden state acts as a store of previous inputs and produces useful context for prediction. Deep RNNs use multiple levels of hidden layers, each with nodes that learn hidden state. As in the case of regular neural network, use of deep RNNs leads to better predictions. If h_t is the current hidden state and h_{t-1} the previous hidden state, w_{hh} , w_{xh} are the weights for connection between hidden states and connection between input and hidden state, respectively, w_{hy} is the weight at output and hidden layer, h_t and y_t is given by Eq. (1), (1) (Fig. 4).

$$h_t = f(w_{hh}h_{t-1} + w_{xh}x_t) \tag{1}$$

$$y_t = w_{hy}h_t \tag{2}$$

As we can see in the above equations provided, the weight w_{hh} is multiplied with previous hidden state. This regulates the strength of the previous hidden state, thereby regulating how much current output is effected by previous hidden states. w_{xh} in a similar fashion dictates the strength of current input. The resultant hidden state computed by Eq. (2) is a linear combination of previous and current input, which helps maintain inter-dependency between inputs. The output is based on the value from the hidden state, which has context from previous inputs stored by hidden states. Instead of using a standard RNN, we are using a LSTM which is a variant

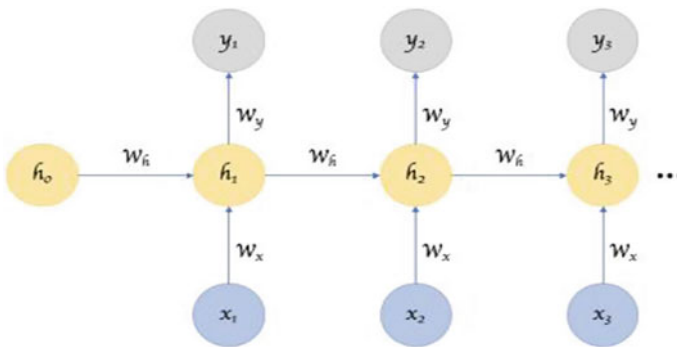


Fig. 4 RNN unrolled in time. *Source* <https://towardsdatascience.com/recurrent-neural-networks-d4642c9bc7ce>

Table 1 Comparison with different models

Title	Predicted DDoS	Predicted not DDoS
Our paper	9092	2273
Hyun Min [11]	11,354	12
<i>K</i> -nearest neighbour (<i>k</i> = 5)	9045	2501
Naive Bayes	7387	3978

Results for *K*-nearest neighbour and Naive Bayes were taken from [11] based on the error rates provided

of RNN. It maintains long range dependencies but also learns better features. It is connected to a sigmoid layer to detect if there is an intrusion (Table 1).

5 Experiments

The model is trained on the CAN intrusion dataset [11]. The dataset contains 3,665,771 ddos messages. We sample the points around the intrusion points in the range of $(-100, 100)$ to build a new dataset to capture the dependencies. With this dataset we trained our LSTM based IDS model to predict DoS attack. We achieved around 80% accuracy. We have shown our model compared to the model discussed in [11]. Our model performed fairly well even though we use less no of parameters to train the model. The comparison results shown reflect our model does better than KNN, Naiver Bayes models. We show out the total no. of DDoS attack in the dataset, how many messages were actually detected as DDoS and how many falsely classified. Overall our model can detect DDoS attacks well but require further exploration to produce high precision.

6 Discussion

We have introduced a IDS system for detecting DoS attack in CAN. Our model uses LSTM with less no of parameters to detect the intrusion. Our model performed fairly when trying to detect intrusion compared to other models. It is a simple model and can be deployed even on low end machines and can be run at a decent speed.

References

1. Leen G, Heffernan D (2002) Expand Automotive Electron Syst Comput 35(1):88–93
2. Stanton NA, Young M, McCaulder B (1997) Drive-by-wire: the case of driver workload and reclaiming control with adaptive cruise control Saf. Sci 27(2):149–159

3. Kim S-H, Seo S-H, Kim J-H, Moon T-M, Son C-W, Hwang S-H, Jeon JW (2008) A gateway system for an automotive system: LIN, CAN, and FlexRay. In: 6th IEEE international conference on industrial informatics, 2008, INDIN 2008. IEEE, pp 967–972
4. Farsi M, Ratcli K, Barbosa M (1999) An overview of controller area network comput. Control Eng. J. 10(3):113–120
5. Miller C, Valasek C (2015) Remote exploitation of an unaltered passenger vehicle. Black Hat USA
6. Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, Koscher K, Czeskis A, Roesner F, Kohno T et al (2011) Comprehensive experimental analyses of automotive attack surfaces. In: USENIX security symposium. San Fran-cisco, pp 77–92
7. Hoppe T, Kiltz S, Dittmann J (2011) Security threats to automotive CAN networks/practical examples and selected short-term countermeasures. Reliab Eng Syst Saf 96(1):11–25
8. Ishtiaq Roufa RM, Mustafaa H, Travis Taylora SO, Xua W, Gruteserb M, Trappeb W, Seskarb I (2010) Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. In: 19th USENIX security symposium. Washington, DC, pp 11–13
9. Szilagy C, Koopman P (2010) Low cost multicast authentication via validity voting in time-triggered embedded control networks. In: Proceedings of the 5th workshop on embedded systems security. ACM, p 10
10. Cyber-security for the controller area network (CAN) communication protocol (2012) International conference on cyber security (CyberSecurity). IEEE, pp 1–7
11. Song HM, Woo J, Kim HK (2020) In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Commun 21:100198
12. Miller C, Valasek C (2013) Adventures in automotive networks and control units. DEF CON 21:260–264
13. Muter M, Asaj N (2011) Entropy-based anomaly detection for in-vehicle networks. In: Intelligent vehicles symposium (IV), 2011 IEEE. IEEE, pp 1110–1115
14. Larson UE, Nilsson DK, Jonsson E (2008) An approach to specification-based attack detection for in-vehicle networks. In: Intelligent vehicles symposium, 2008 IEEE. IEEE, pp 220–225
15. Song HM, Kim HR, Kim HK (2016) Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network. In: 2016 international conference on information networking (ICOIN). IEEE, pp 63–68
16. Cho K-T, Shin KG (2016) Fingerprinting electronic control units for vehicle intrusion detection. In: 25th USENIX security symposium (USENIX Security 16). USENIX Association, pp 911–927
17. Kang M-J, Kang J-W (2016) Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE 11(6), Article e0155781
18. Seo E, Song HM, Kim HK (2018) GIDS: GAN based intrusion detection system for in-vehicle network 2018 16th Annual Conference on Privacy, Security and Trust (PST). IEEE, pp 1–6
19. Wang C, Zhao Z, Gong L, Zhu L, Liu Z, Cheng X (2018) A distributed anomaly detection system for in-vehicle network using HTM. IEEE Access 6:9091–9098
20. Levi M, Allouche Y, Kontorovich S (2018) Advanced analytics for connected car cyber-security. In: 2018 IEEE 87th vehicular technology conference (VTC Spring). IEEE, pp 1–7
21. Chandola V, Banerjee A, Kumar V (2012) Anomaly detection for discrete sequences: a survey. IEEE Trans Knowl Data Eng 24(5):823–839
22. Xing Z, Pei J, Keogh E (2010) A brief survey on sequence classification. ACM SIGKDD Explor Newsl 12(1):40–48
23. Hofmeyr SA, Forrest S, Somayaji A (1998) Intrusion detection using sequences of system calls. J Comput Secur 6(3):151–180
24. Kosoresow AP, Hofmeyer S (1997) Intrusion detection via system call traces. IEEE Softw 14(5):35–42
25. Lee W, Stolfo SJ, et al (1998) Data mining approaches for intrusion detection. In: USENIX security symposium. San Antonio, TX, pp 79–93

26. Ou C-M (2012) Host-based intrusion detection systems adapted from agent-based artificial immune systems. *Neurocomputing* 88:78–86
27. Shabtai A, Kanonov U, Elovici Y, Glezer C, Weiss Y (2012) \Andromaly: a behavioral malware detection framework for android devices. *J Intell Inf Syst* 38(1):161–190
28. Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: methods, systems and tools. *IEEE Commun Surv Tutor* 16(1):303–336
29. Yu SJ, Koh P, Kwon H, Kim DS, Kim HK (2016) Hurst parameter based anomaly detection for intrusion detection system. In: 2016 IEEE international conference on computer and information technology (CIT). IEEE, pp 234–240
30. Wang W, Zhu M, Zeng X, Ye X, Sheng Y (2017) Malware traffic classification using convolutional neural network for representation learning. In: 2017 international conference on information networking (ICOIN). IEEE, pp 712–717

Analysis of Fuel Cell—Battery and Supercapacitor in Driving the Integrated UPQC



Vodapalli Prakash

Abstract Unified Power Quality Conditioner (UPQC) is a versatile conditioning device to improve the perturbances in the power network. Here executed the performance of fuel cell-battery-integrated UPQC with supercapacitor to mitigate the power problems for unbalanced loads. The given method clarifies how best the integrated system works whenever sudden disturbances occurred in the system. The system is the mixture of a DC-to-DC converter fed by a fuel cell unit along with battery worked as the supplementary power device at the DC link to meet the conditions at the suitable point. A proper control mechanism is utilized for observing the system conditions, and it is implemented with MATLAB.

Keywords Supercapacitor · Fuel cell · Capacity · UPQC · Harmonic distortion · Voltage variations

1 Introduction

The customers are forced to use wide variety of power electronic equipment due to automation of the work everywhere. Every day the ratio of nonlinear elements are increasing in the overall system. The urban segment is increasing at the same time shopping area, malls, IT hubs and commercial points with different load requirements. The forecasting of load on the system becomes a headache for the engineers with respect to time [1].

The latest equipment are almost of digital type and slowly inject unwanted signals and spoil the network. With the involvement of these devices continuously may cause disturbances. If the supply deviates from the ideal supply conditions leads to damage and not proper working of equipment or malfunctioning at the customer end [2–6]. In the custom devices, UPQC is one of the trusted devices in compensating the problems. UPQC combines the series as well shunt filters connected back to the back on the DC side. It utilizes two voltage source inverters to along with a DC

V. Prakash (✉)

Kakatiya Institute of Technology and Science, Warangal, T.S, India
e-mail: vp.eee@kitsw.ac.in

capacitor. The series filters are considered for enhancing the voltage—profiles and reducing harmonics. Shunt filter [7–9] is used to take care of currents. FCs are capable of transforming chemical into electrical energy. Super capacitors and fuel cells are used in defence sectors, toys, hybrid electric vehicles and for various commercial and industrial sectors as well as used in remote applications [10–12]. Fuel cell has little maintenance as well as less pollution. Depending upon the load requirements fuel cells can be arranged, especially at the starting moments and unwanted faults may happened in the system [13, 14]. Depends on the size, the ratings need to be changed and reduces the cost also employing the fuel cell alone [15–17]. Addition of battery decreases the burden on the fuel cell also enhances the system functional capacity and overloading [18]. The fuel cell with battery used in the DC link for short bit of time and parallelly enhances the FC dynamics. During peak time, fuel cell injects the current along with battery current and supports peak demand periods. The DC-to-DC converter considered as buck–boost converter employed in the system to handle the voltage sag and swells [19, 20].

The permitted THD of the source current is less than 5% based on IEEE 519–1992 standards [21, 22]. This integrated supercapacitor with fuel cell-battery (SCFCB) unit is managed to enhance the working capacity of UPQC, DC/DC converter. The execution depicted as: Sect. 1 gives the introductory part explains the present scenario of system with combinational loads and their significance in power quality, Sect. 2 describes about the fuel cell-battery-integrated UPQC, Sect. 3 depicts the series and shunt active power filters and their control and DC-DC converter. Section 4 shows the results with integrated FCB with and without battery. Section 5 adds conclusion part.

2 SCFCBS-Integrated UPQC

The integrated UPQC with supercapacitor and fuel cell-battery unit configuration shown in Fig. 1. The active filters are employing a DC link given to a fuel cell battery unit given to the DC capacitor, where battery uses as the short energy backup facility for long term to maintain stability for critical loads. In this approach, $d-q$ method is used for the FCB-integrated UPQC with a DC-to-DC converter to manage the voltages at the fuel-cell unit to get expected result. It uses Park's and Inverse Park's transformation for the creation of the reference signal.

3 Supercapacitor Fuel Cell—Battery (SCFCB) Integrated UPQC

Fuel cells are producing electricity by taking chemical energy as input. Out of the FC's, PEMFC is widely used due to its flexible applications, very easy start up and

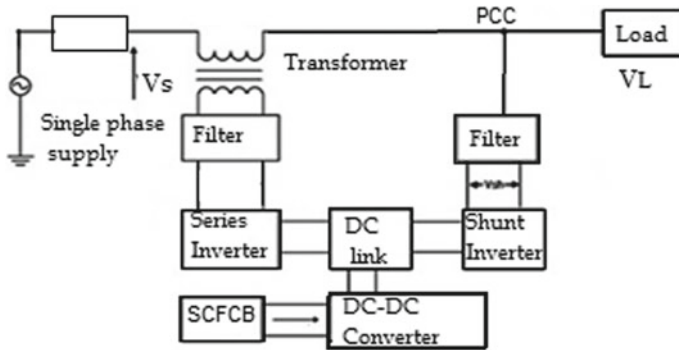


Fig. 1 SCFCB-integrated UPQC [23]

used for low-temperatures and corrosion problems are minimal [22], it is shown in Fig. 5.

3.1 Series APF

The target of this is to eliminate harmonics, shown in Fig. 3, employed to suppress voltage harmonics. It is also be applied to regulate the voltage imbalances in the systems [23]. The phase voltages are collected and given to point of common coupling which generates angles $(\sin\theta, \cos\theta)$.

The components of voltages in d - and q -axes are shown in Eqs. (1) and (2)

$$V_{dh} = V_{dDC} + V_{dAC} \tag{1}$$

$$V_{qh} = V_{qDC} + V_{qAC} \tag{2}$$

V_{dh} , V_{qh} are d -axis and q -axis voltages consist of DC (fundamental), ripple (harmonic) components and V_{dDC} , V_{qDC} are direct-axis and quadrature-axis fundamental DC voltages. The ref. d - and q -axis voltages are V_d^* , V_q^* are given by,

$$V_d^* = V_{dDC} - V_o \tag{3}$$

$$V_q^* = V_{qDC} + V_{qr} \tag{4}$$

The two reference voltage values (V_d^* , V_q^*) are used to generate the reference load voltages, to adjust the amount of voltage at series APF. The Inverse Park transformation is applied for producing the reference voltages.

3.2 Shunt Converter

Shunt APF is shown in Fig. 4 targeted to control the link voltage as well and to compensate the load current under reactive, non-linear loads. The I_d^* , I_q^* values are

$$I_d^* = i_{dDC} + i_{out} \tag{7}$$

$$I_q^* = i_{qDC} + i_{qr} \tag{8}$$

where i_{dDC} , i_{qDC} direct-axis and quadrature-axis fundamental currents, i_{out} is the output of the PI controller. The working voltage of the fuel cell varies like 65-75 V, while the DC link voltage is about 670 V.

4 SCFCB—Results Analysis

Figure 2 shows the combined FCB—UPQC demonstrates a sag in the source end-voltage from 0.2 to 0.4 s displayed. The source voltage, load side voltage, magnitude of injected voltage, the UPQC can correct the voltage related problems to make the load voltage is normal. There is no additional device is needed to improve the power factor (Fig. 3).

A voltage swell is observed from 0.2 to 0.4 s in the source voltage, and the after mitigation, the load voltage is maintained constant, it is shown in Fig. 2b.

The UPQC is corrected the load reactive power, whenever there is a sudden disturbance. Figure 4 shows the stabilization of DC link voltage.

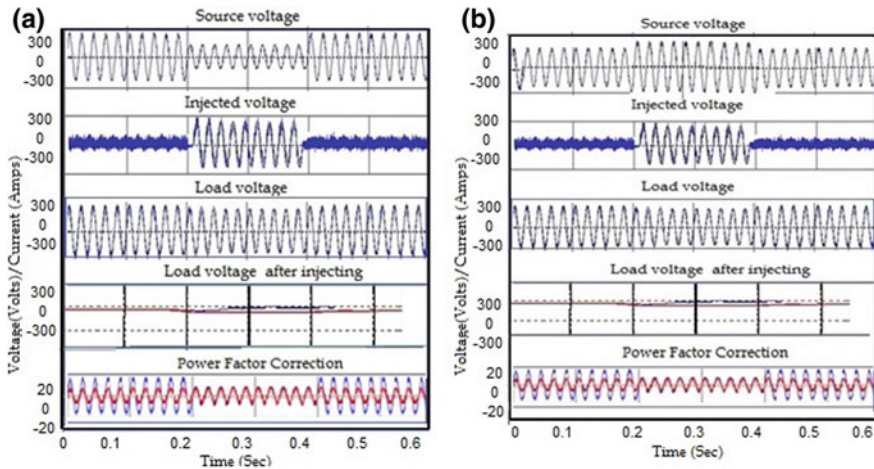


Fig. 2 a Sag compensation. b Swell compensation

Fig. 3 Current waveforms

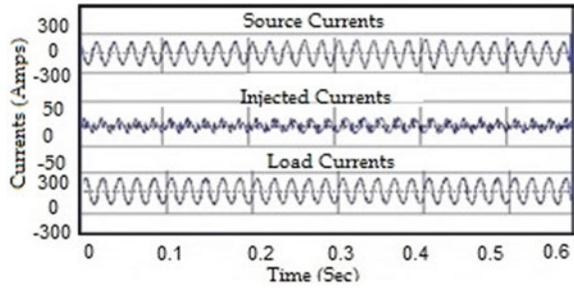


Fig. 4 DC link voltage

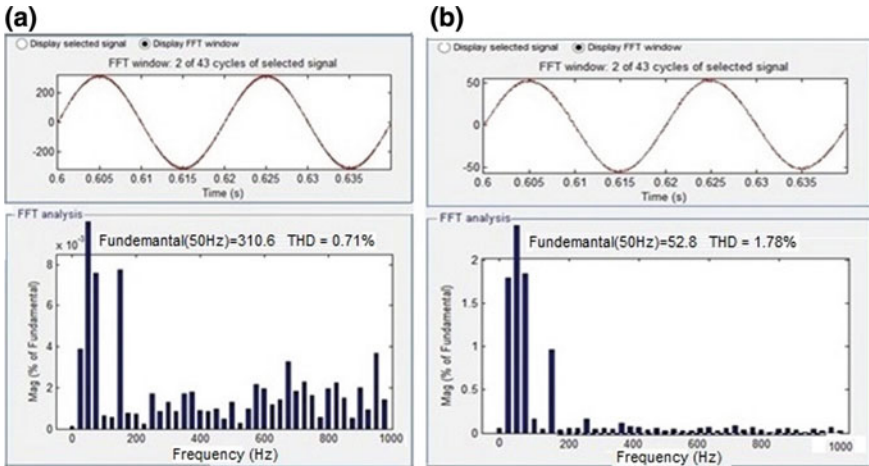
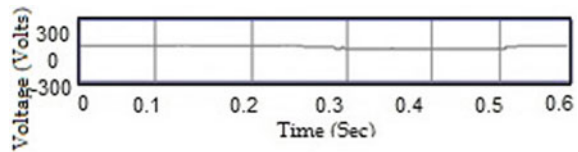


Fig. 5 a Source current. b Load voltage

Figure 5a and b represents the harmonics of source current, load voltage. The THD of the source current and load voltage values are 0.71 and 1.78%, respectively.

5 Conclusion

This paper concentrated on the working performance of fuel cell battery with supercapacitor combined single-phase UPQC implementation, which includes the different

compensating capabilities. In this, fuel cell performing well in mitigating voltage sag, swells and power factor correction without using an additional device. This composition perfectly handles the problems associated with voltage and currents. In the practical scenario due to automation, everyone is forced to use various power electronic devices which in turn possess the nonlinear behaviour. As a result, harmonic content is slowly introduced in to the network. As a result, different problems may arise in the network. The controlling technique is managed THD values effectively as per IEEE tables. The THD of source current is less when compared to supercapacitor for the same system executed through MATLAB systems.

Acknowledgements I thank Head Dr. C.Venkatesh and Principal Dr. K. Ashoka Reddy and Management KITSW for their support and motivation.

References

1. Han BM, Bae B (2008) Unified power-quality conditioner with super-capacitor energy storage. *Euro Trans Electr Power* 18:327–343
2. Kesler M, Ozdemir E (2009) Simplified control method for unified power quality conditioner (UPQC). *Int Conf Renew Energies Power Q* 1(7):474–478
3. Argyrou M, Christodoulides P, Marouchos C, Kalogirou S (2018) Hybrid battery-supercapacitor mathematical modeling for PV application using Matlab/Simulink. <https://doi.org/10.1109/UPEC.2018.8541933>, (2018)
4. Khalid S, Dwivedi B (2011) *Int J Adv Eng Technol* 1(2):1–11
5. Paladini V, Donateo T, de Risi A, Laforgia D (2007) Super-capacitors fuel-cell hybrid electric vehicle optimization and control strategy development Elsevier. *Energy Conver Manage* 48:3001–3008
6. Moreno VM, Pigazo A, Liserre M, Dell'Aquila A (2008) Unified power quality conditioner (UPQC) with voltage dips and over-voltages compensation capability. <https://doi.org/10.24084/repqj06.28>
7. Ganguly S (2014) Impact of unified power-quality conditioner allocation on line loading, losses, and voltage stability of radial distribution systems. *IEEE Trans On Power Delivery* 29(4):1859–1867
8. Axente I, Ganesh JN, Basu M, Conlon MF, Gaughan K (2010) A 12-kVA DSP-controlled laboratory prototype UPQC Capable of mitigating unbalance in source voltage and load current. *IEEE Trans Power Electron* 25(6):1471–1479
9. Yu X, Starke MR, Tolbert LM, Ozpineci B (2007) Fuel cell power conditioning for electric power applications: a summary. *IET Electric Power Appl* 1(5):643–656
10. Eltamaly AM, Sayed Y, Abou-Hashema M, El-Sayed, Elghaffar ANA (2019) Voltage sag compensation strategy using dynamic voltage restorer for enhance the power system quality. *J Electric Eng* 3(19). ISSN No: 1582-4594
11. Nanda B, Jena RK (2019) Performance of battery bank on hybrid microgrid. *Int J Electric Eng Technol (IJEET)* 10(3):56–63
12. Liu H, Chen J, Hissel D, Lu J, Hou M, Shao Z (2020) Prognostics methods and degradation indexes of proton exchange membrane fuel cells: a review. *Renewable Sustaina Energy Rev* 123:109721. ISSN 1364-0321. <https://doi.org/10.1016/j.rser.2020.109721>
13. Gou B, Na WK, Diong B (2010) Fuel cells modeling, control and applications. CRC Press, pp 02

14. Allou N, Abdelmalek D, Fetha C (2016) Analysis of Electric disturbances in the quality of electric energy using the ABC method of classification for the application to voltage dips and short interruptions. *J Electric Eng* 4edn, 16(4), Article 16.4.12
15. Jayalakshmi NS, Nempu PB, Shivarudraswamy R (2016) Control and power management of stand-alone PV-FC-UCHYBRID system. *J Electric Eng*
16. Onar OC, Uzunoglu M, Alam MS (2008) Modeling, control and simulation of an autonomous wind turbine/photovoltaic/fuel cell/ultra-capacitor hybrid power system. *J Power Sources* 185:1273–1283
17. Satpathya S, Dasa S, Bhattacharyyab BK (2020) How and where to use super-capacitors effectively, an integration of review of past and new characterization works on super-capacitors. *J Energy Stor.* <https://doi.org/10.1016/j.est.2019.101044>
18. Stanley Whittingham M, Savinell RF, Zawodzinski T (2004) Guest editors. *Batteries Fuel Cells* 104(10)
19. Vodapalli P, Rama Subba Reddy T, Tara Kalyani S, Karandikar PB (2014) Application of supercapacitor in enhancing power quality of UPQC for three phase balanced/unbalanced loads. *J Electric Eng* 4(14). ISSN No: 1582-4594
20. Zhang Y, Zhang S, Chen J (2008) The applications of bidirectional full-bridge DC-DC isolated converter in UPQC. *International conference on electrical machines and systems. Wuhan*, pp 1916–1919
21. *Fuel Cell Handbook (Fifth Edition) (2000) By EG&G Services Parsons, Inc. Science Applications International Corporation*, pp 1–3
22. Kim Y, Kim S (1999) An electrical modeling and fuzzy logic control of a fuel cell generation system. *IEEE Trans Energy Conver* 14(22):239–244
23. Singh B, Chandra A, Al-Haddad K (2015) *Power quality: problems and mitigation techniques. WILEY, ISBN: 978-1-118-92205-7*

A Compact Microstrip Antenna with DGS for Bluetooth Applications



M. Chandra Sekhar, M. Suneel Raja, B. Sai Varshini, A. Gunapreetham, K. Neha, and G. Vishal

Abstract This paper presents a compact patch antenna operating in S-band frequency which is etched with a triangular dumbbell-shaped defected ground structure has been proposed for Bluetooth applications. The antenna uses inset feeding technique and RT duroid as substrate holding relative permittivity of 2.2. The patch antenna parameters have been compared before and after installing DGS, namely return loss, gain, and VSWR. The results have shown that antenna parameters and performance have been improved drastically after installing DGS. The high frequency structured simulator software (HFSS) has been assigned for simulations and to obtain parameters like voltage wave standing ratio, return loss, gain, bandwidth, and current distribution. The radiation pattern for co-polarization and cross-polarization, in both magnetic plane and electrical plane of the designed antenna, is also presented. The depicted antenna has a return loss less than 10 dB and VSWR less than 2 and provides a very good bandwidth. The depicted antenna is fabricated and the practical results are analyzed. It shows that the simulated results and the measured results are almost same.

Keywords Microstrip antenna · Triangular dumbbell DGS · Inset feed · Bluetooth application

1 Introduction

In this day-to-day advancing world driven mainly by technology and its applications, communication has become one of the most needed things for our lives to keep up with the current running world. Ever since the communication technology has gained its prominence many devices and technologies have been introduced in the market

M. Chandra Sekhar (✉) · M. Suneel Raja
Department of ECE, Kakatiya Institute of Technology and Science, Warangal, T.S, India
e-mail: mc.ece@kitsw.ac.in

B. Sai Varshini · A. Gunapreetham · K. Neha · G. Vishal
Kakatiya Institute of Technology and Science, Warangal, T.S, India

to improve the effectiveness of our communication and to decrease the time delay. One of very first technologies which have gained a good prominence in short-range wireless communication is Bluetooth technology [1–3]. Ever since the Bluetooth technology and devices got introduced in the market, it is continuing to serve the need for communication and has not lost its prominence till today. Many advancements were also brought in improving the Bluetooth technology and to make it effective and improve its performance. A microstrip antenna is a compact size, less weight, and directional antenna mostly known for its low cost, low profile, portability, ease of manufacturing, its adaptivity with integrated circuits, and its simplicity in installing over any surface [4, 5].

Despite choosing the best suitable substrate, feeding technique, and calculating accurate patch dimensions for the antennas, there is still a drawback in antenna parameters so we switched to a new design by introducing a triangular dumbbell slot [6–8]. The rectangular patch antenna embedded defected ground has been assigned for Bluetooth applications. The defected ground structure (DGS) is a miniaturization technique which means there can be considerable reduction in antenna size and weight. The antenna size is reduced to a greater extent by implementing DGS [9, 10]. Several compact antennas are implemented using fractals concept [11–15]. A compact S-band microstrip antenna is designed in this paper embedded with a triangular dumbbell-shaped DGS using inset feeding technique for Bluetooth applications. By making use of defected ground structure, the antenna has resonated at desirable frequency and provided with sufficient gain, VSWR, and bandwidth. The upcoming section, i.e., Sect. 2 describes antenna design and its required equations, Sect. 3 represents the simulated and real-time analyzed results and finally Sect. 4 provides conclusion and results of the depicted compact microstrip patch antenna.

2 Antenna Outline and Equations

The measurements of the rectangle shape microstrip antenna are displayed in Fig. 1. The patch antenna uses RT duroid having relative permittivity of 2.0.2 as substrate with dimensions $82.1 \times 82.1 \times 1.57 \text{ mm}^3$. The rectangular patch antenna with triangular dumbbell-shaped DGS is drafted to resonate at Bluetooth frequency. The dimensions of the designed patch antenna are patch dimensions is $48.4 \times 40.5 \text{ mm}$, substrate length and width is $82.1 \times 82.1 \text{ mm}^2$ and length of inset feedline is 24.929 mm. Those are some of the important equations and dimensions which have been derived using them for the proposed antenna. Now coming to basic layout of the designed microstrip antenna which is displayed in Fig. 1.

Figure 2 displays the measurements of the depicted antenna ($82.1 \times 82.1 \text{ mm}$) whose patch length is 48.4 mm and patch width is 40.5 mm. The substrate thickness is 1.57 mm. The inset feedline is provided with a length and width of 36.65 and 4.85 mm, respectively. This initial antenna is simulated and the results obtained looked like there is a need for improvement. Then the DGS structure is etched in the ground. The triangular dumbbell slot in the ground has greatly improved the antenna

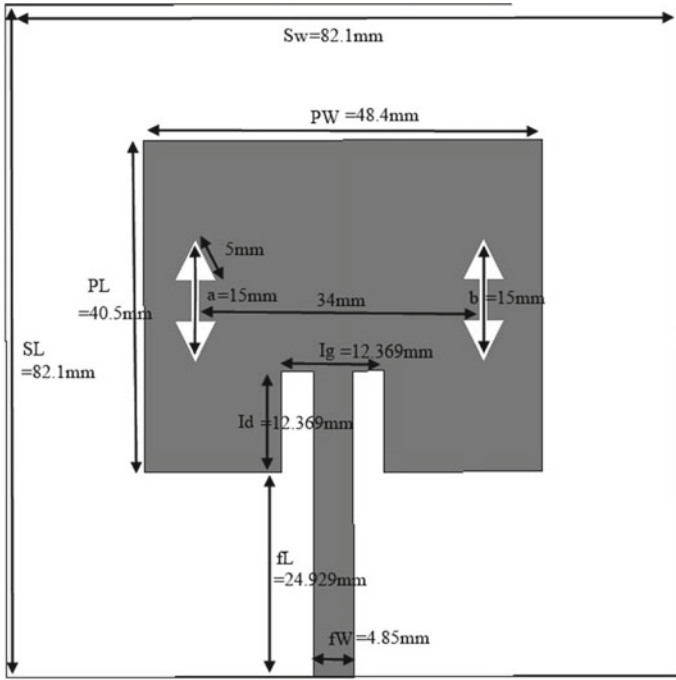


Fig. 1 Dimensions of the proposed antenna

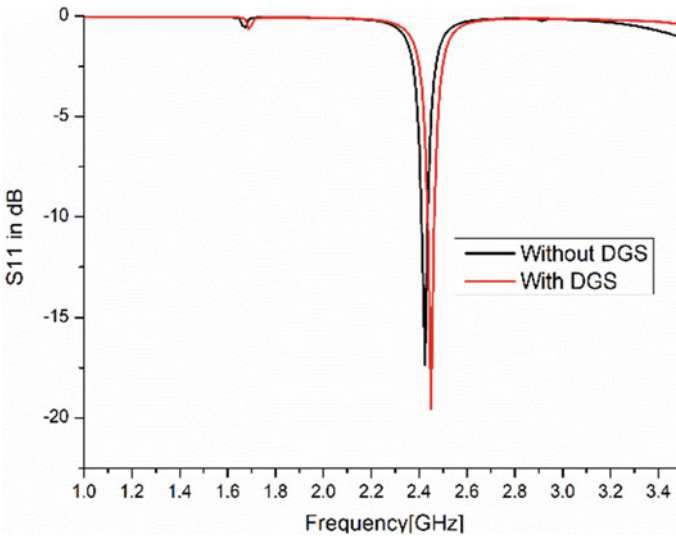


Fig. 2 Return loss plot estimation for antenna with and without DGS

parameters. The triangular dumbbell DGS slot etched in the ground which greatly improved the antenna performance and all the dimensions of the depicted Fig. 1 are in mm.

3 Simulations and Results

The above proposed dimensions of the antenna along with DGS have been in high frequency structured simulator (HFSS) software and obtained the desired results. The depicted antenna's return loss which is S-parameter Vs Frequency curve is displayed in Fig. 2.

The depicted antenna's return loss is obtained as 19.5 dB with DGS and increased by 2.5 when compared with the one without DGS. Now coming to another important parameter of the antenna, i.e., overall gain between both the designs, i.e., with and without DGS of the depicted antenna is presented in Fig. 3.

The cross-polarization and co-polarization pattern in H-plane and E-plane for the depicted rectangle-shaped patch antenna with and without DGS is depicted in Fig. 4 which had been simulated in HFSS.

The current distribution in a patch antenna is mostly dependent on substrate's height and what kind is being used. The current distribution along the depicted antenna, i.e., both bottom and top of the patch is shown in Figs. 5 and 6.

From Fig. 6, we can see at the center of the patch, the current distribution is maximum at the resonating frequency, i.e., 2.45 GHz. The modeled antenna is now

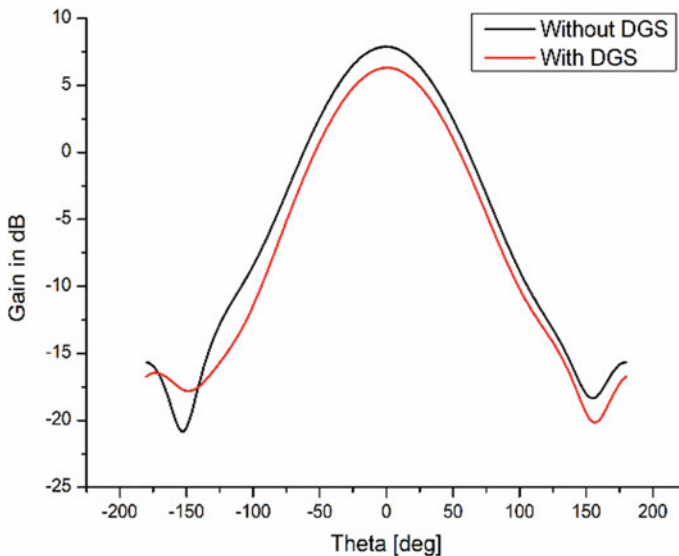


Fig. 3 Estimation of gain plot for antenna with and without DGS

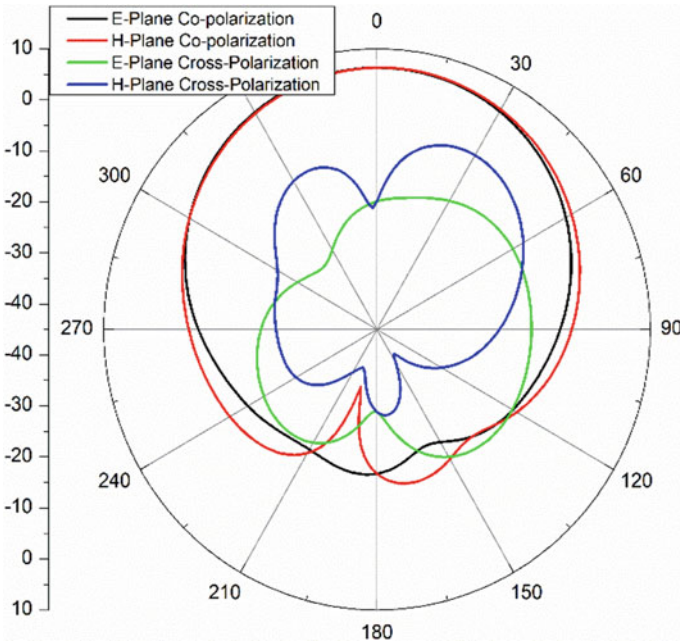


Fig. 4 Cross-polarization and co-polarization pattern for proposed antenna with DGS

fabricated and tested to cross-check whether the simulated results and actual results are similar or not. In order to increase the compatibility with other devices and to see the range of connection, the fabricated real-time antenna is shown in Fig. 7.

Now, the antenna is fabricated and the analyzed results are obtained. The simulated antenna results have been compared with that of fabricated one. The two main antenna parameters are being compared between simulated and real-time observed results. Those main parameters are return loss and VSWR. Figure 8 represents the return loss comparison plot between simulated and fabricated results.

From Fig. 8, we can notice that return loss curve for simulated and measured is similar and has not been deviated much. Now the VSWR plot between simulated and measured results is shown in Fig. 9.

In Fig. 9, we can see that the VSWR curves for both simulated and measured results were almost the same. So, as the return loss plot and VSWR plot did not shown much difference the antenna designed and fabricated can be utilized for Bluetooth applications. Various comparison tables have been prepared based on different parameters and among various designs of antenna, i.e., with and without DGS and among various references and proposed design (Tables 1, 2 and 3).

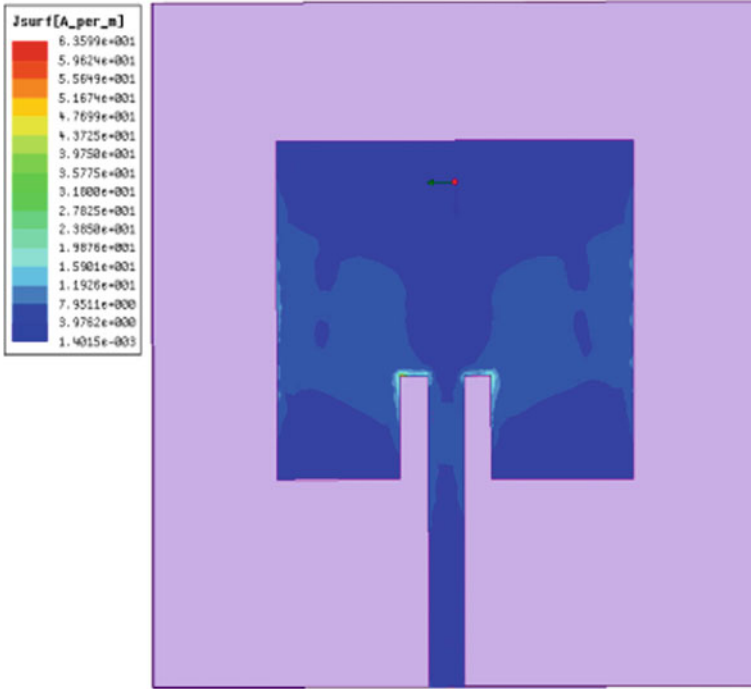


Fig. 5 Depicting the current distribution on top of the patch in the proposed antenna

4 Conclusion

The rectangular patch antenna has been proposed with inset feeding technique and triangular dumbbell-shaped defected ground structure to operate at Bluetooth frequency (2.45 GHz). This DGS has been installed for the miniaturization of antenna, to improve antenna parameters and to reduce overall size. The antenna is simulated in HFSS which is designed using the design equations and the practical results have been analyzed using the network analyzer. The depicted antenna with a triangular dumbbell-shaped DGS exhibits a return loss of 19.55db, VSWR of 1.38, bandwidth of 60 MHz, and satisfactory gain. The results of antenna with DGS and without DGS have been compared and it turns out that the antenna with DGS have greatly improved in parameters like gain, VSWR, bandwidth and became compact in size. This unique design of triangular dumbbell-shaped DGS antenna has significantly improved its efficiency and can be applied for Bluetooth applications.

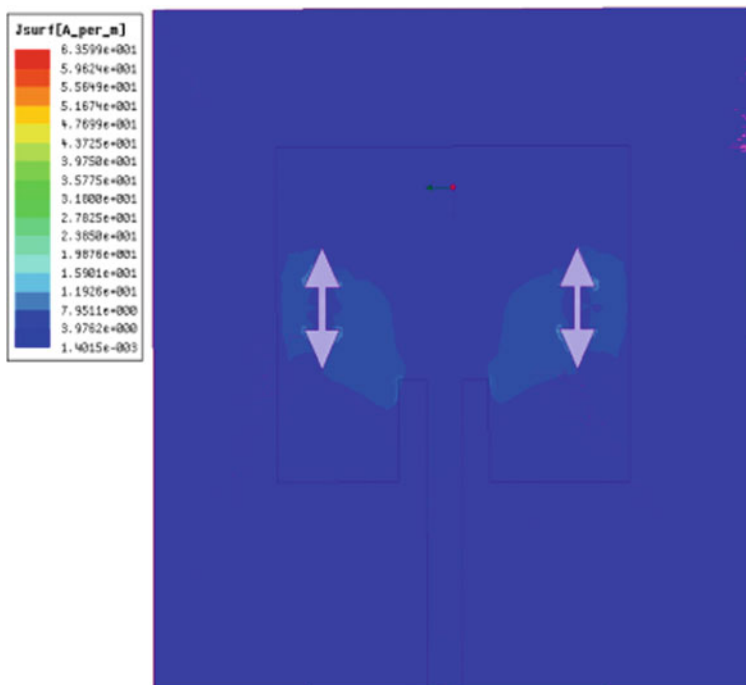


Fig. 6 Current distribution at the back of the patch for the designed microstrip antenna

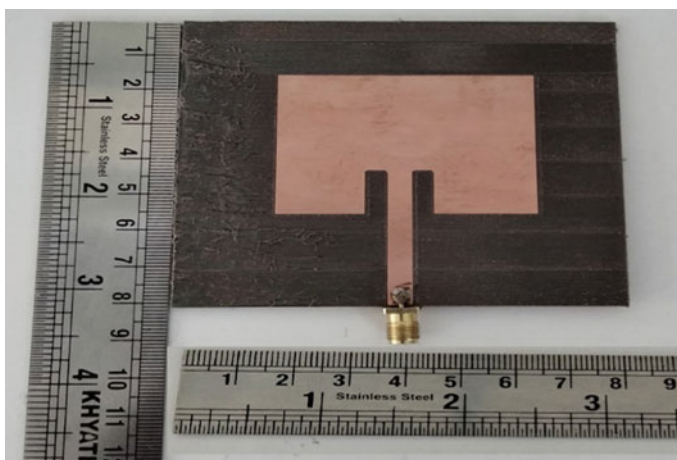


Fig. 7 Representing the patch of the fabricated antenna

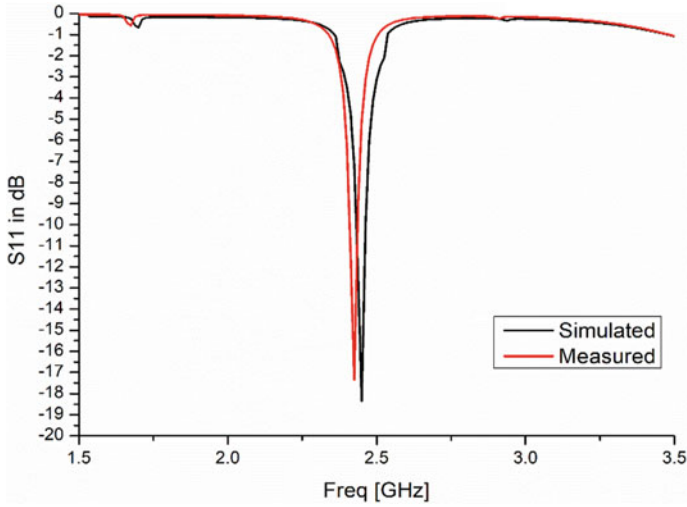


Fig. 8 Return loss for simulated and measured antenna

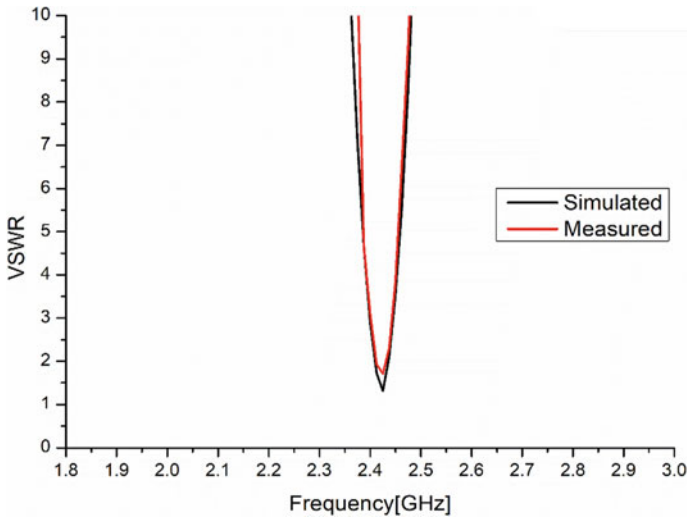


Fig. 9 VSWR for simulated and measured antenna

Table 1 Comparison of antenna parameters with and without DGS

Type of antenna	Frequency (GHz)	Return loss (dB)	VSWR	Gain (dB)	Bandwidth (MHZ)
Without DGS	2.44	-17.33	1.27	7.83	48
With DGS	2.45	-19.55	1.38	6.33	60

Table 2 Comparison of antenna results in HFSS and real-time results

Parameters of the depicted antenna	Return loss (db)	VSWR
Simulated results	-19.5	1.27
Measured results	-17.8	1.54

Table 3 Comparison of different antenna designs for Bluetooth applications

References No.	Size	Patch shape	DGS	Return loss (db)	Bandwidth (MHz)	VSWR	Type of feed
[6]	58.53 × 56.53 mm	Rectangle	U shaped	-15.9	25	1.38	Microstrip feedline
[7]	60 × 50mm	Rectangle	Ring shaped	-14.06	30	1.42	Microstrip feedline
[8]	200 × 200mm	Wang shape	-	-16	42	1.4	Probe feeding
Designed antenna	82.1 × 82.1 mm	Rectangle	Triangular dumbbell shaped	-19.5	60	1.38	Inset feedline

Acknowledgements This work has been reinforced by the Science and Engineering Research Board (SERB), New Delhi, India (Grant No.: EEQ/2017/000118).

References

1. Bod M, Hassani HR (2012) Compact UWB printed slot antenna with extra bluetooth, GSM, and GPS Bands. *IEEE Antennas Wireless Propag Lett* 11
2. Abd-Elrazzak MM, Member, IEEE, AI-Nomay IS (2013) A design of a circular microstrip patch antenna for bluetooth and HIPERLAN applications. *IEEE Antennas Wireless Propag Lett*
3. Ghosh I, Roy JS (2007) Performances of two dual-frequency microstrip antennas for GPS and bluetooth communications. *IEEE*
4. Vyshnavi Devi G, Pramodh Kumar K (2017) Design of a simple slotted rectangular microstrip patch antenna for bluetooth applications. *IRJET* 4(3)
5. Thamizhazhagi R, Abirami D (2015) To design and analyse the performance of microstrip ring slot antenna for 2.4GHz. In: *IJERT*, ISSN:2278-0181, NCEASE
6. Chandan BSR (2014) Dual-band wang shaped microstrip patch antenna for GPS and bluetooth application. In: 2014 sixth international conference on computational intelligence and communication networks.
7. Lu L, Coetzee JC (2005) Reduced-size microstrip patch antenna forBluetooth applications. *IEEE Electron Lett* 41(17)
8. Dongre V, Mishra A (2016) Design of single band and dual band microstrip antennas for GSM, GPS and bluetooth applications. In: International conference and workshop on electronics and telecommunication engineering
9. Dhruv S, Diksha P (2016) Microstrip patch antenna for Wi-Fi and bluetooth application in the ISM band. *IJRES* 20

10. Sontakke M, Savairam V (2017) Microstrip patch antenna with DGS for Bluetooth application. *IJRET* 6(3)
11. Reddy VV, Sarma NVSN (2017) Single layer single probe feed circularly polarized triple band fractal boundary microstrip antenna for wireless applications. *Int J Microw Wirel Technol* 9(3):657–664
12. Reddy VV (2019) Frequency reconfigurable fractal patch circularly polarized antennas for GSM/Wi-Fi/Wi-MAX applications. *IETE J Res* 1–8
13. Reddy VV (2018) Broadband Koch fractal boundary printed slot antenna for ISM band applications. *Adv Electromagnet* 7(5):31–36
14. Reddy VV, Sarma NVSN (2016) Reactive impedance surface-based broadband circularly polarized Koch fractal boundary microstrip antenna. *Int J Microw Wirel Technol* 8(2):243–250
15. Reddy VV (2021) Metamaterial loaded circularly polarized fractal antenna for 2.4 GHz frequency applications. *IETE J Res* 1–10

A Circularly Polarized Single-Feed Patch Antenna for C-Band Satellite Applications



M. Chandra Sekhar, M. Suneel Raja, and Shaik Samreen Sultana

Abstract Designing of a probe-fed wideband square patch antenna is presented to satisfy the applications of a C-band satellite. An antenna with optimal performance is developed utilizing a RT Duroid substrate with single feed and dielectric constant of 2.2. Furthermore, adept investigation and adequate determination of the parameters related to the suggested antenna structure is performed. Compatibility of this overall antenna structure is high with respect to the alignment; hence it is of much importance for applications of C-band satellite. By experimentation and simulation, the features of the suggested antenna were examined. Also, it is noticed that the agreement between the measured and simulated results is good. Results of the antenna prototype that are measured exhibit a 10 dB return loss bandwidth of 103 MHz, a 3 dB axial ratio (AR) bandwidth of 50 MHz (1.19%), gain of 6.13 dB at resonant frequency 4.19 GHz, respectively.

Keywords Square patch antenna · Probe feed · Circular polarization · C-band satellite application

1 Introduction

In various wireless communication systems, these circularly polarized antennas (CP) are extensively applied for receiving satellite signals at C-band frequency. As polarization of radio wave that is linearly polarized is exposed to Faraday rotation when it moves in and out of the ionosphere, circularly polarized antennas were employed to avoid any kind of improper alignment between the receiver and the transmitter [1–3]. Furthermore, circularly polarized antennas are more advisable in absence of Faraday rotation as no particular alignment is needed amidst the receiving and

M. Chandra Sekhar (✉) · M. Suneel Raja · S. S. Sultana
Department of ECE, KITSW, Warangal, T.S, India
e-mail: mc.ece@kitsw.ac.in

S. S. Sultana
e-mail: b18ec104@kitsw.ac.in

transmitting antennas for polarization matching, for example, dedicated communication. In comparison with linearly polarized antennas, CP structures [4, 5] are largely employed in satellite communications because they can deliver better weather penetration and mobility.

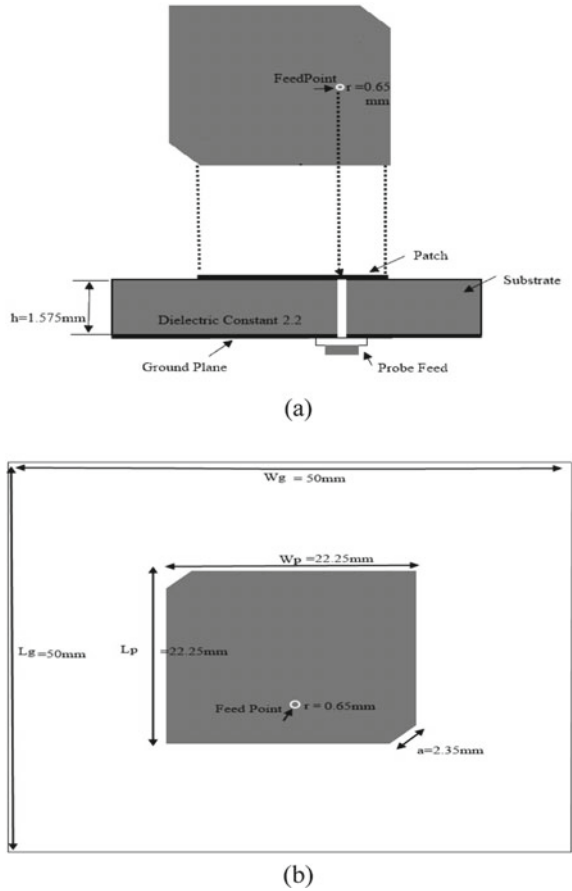
Introducing two 90° out of phase orthogonal signals and equivalent magnitude to the edges of the square patch structure that are non-radiating and radiating is the standard process to [6–8] attain circular polarization (CP). In spite of the excellent axial ratio (AR) and high circularly polarized (CP) bandwidth, the dual-feed method takes up more space on the board and needs an external polarizer. Accordingly, in current years, the single-feed compact CPAs have acquired much priority. Generation of circular polarization (CP) from elements that are aperture coupled can be done utilizing u-slots [5, 9–12] or coupling apertures. Employing x-slots or two slots is revealed to be effective in generating higher 3 dB axial ratio bandwidths, but this needs feed networks consisting mixed cross couplers. For the operation of CP, various single-feed single-layer structures are proposed. Nevertheless, in all these approaches, the 3 dB AR bandwidth that is reported is extremely tapered, while the best AR is higher than 0.5 dB at desired frequency.

Within the paper, a unique circularly polarized antenna configuration is suggested which is established on pruning the edges of a square patch structure using single feed for the applications of C-band satellite. The side and top views of the suggested structure are shown in Fig. 1. The axial ratio (AR), excellent impedance bandwidth, well-defined CP, simplicity and compactness are the novelty of this structure. The content flow of the paper is as follows: the antenna design principle is represented in Sect. 2, the results and discussions are introduced in Sect. 3 and the conclusion is given in Sect. 4.

2 Antenna Design

Figure 1 demonstrates the structure of the suggested single-feed circularly polarized antenna. The patch is to be etched on RT Duriod substrate. The following are the features of the structure that is simulated and resonated at 4.19 GHz: the patch side length (L) is 22.25, 1.575 mm as the substrate thickness (h); relative permittivity as 2.2; 0.0019 as the loss tangent. A single probe feed comprising input impedance of 50Ω is hooked to the patch via hole for stimulating purpose. The effect of inductance because of the conductor that is inside the probe is negated by capacitive coupling of the via. Excitation of double orthogonal modes of phase shift 90° is possible through corner truncation of a single-feed square patch. With a purpose to attain good impedance matching for the antenna structure, feeding position was optimized through considerable simulations. The centre of the patch is moreover not aligned. This is to acquire the appropriate impedance matching inside the desirable frequency band. The corner truncation of the patch plays a key function in accomplishing an AR beneath 3 dB. Photograph of the suggested model is shown in Fig. 2.

Fig. 1 Geometry of suggested model. **a** Side view. **b** Top view



3 Results and Discussion

The HFSS, electromagnetic simulation package, is used to optimize the proposed antenna. This software depends on the finite element method for electromagnetic calculations. The antenna has dimensions of $50 \times 50\text{mm}^2$ while accomplishing an acknowledged gain and radiation effectiveness. Cautious configuring of the corner truncations of the patch is required to obtain good operation of CP for the structure. To improve the CP bandwidth in the desired band, RT Duriod substrate dielectric material is used. Comparison of conventional single-feed circular polarization antennas is given in Table 1. The antenna prototype is then manufactured in the antenna measurement laboratory of KITSW.

Figure 3 illustrates coefficient of reflection that is simulated and computed. The measured and simulated results in C-band have a reasonable agreement. The measured value of impedance bandwidth of 10 dB for C-frequency band is (2.45%),

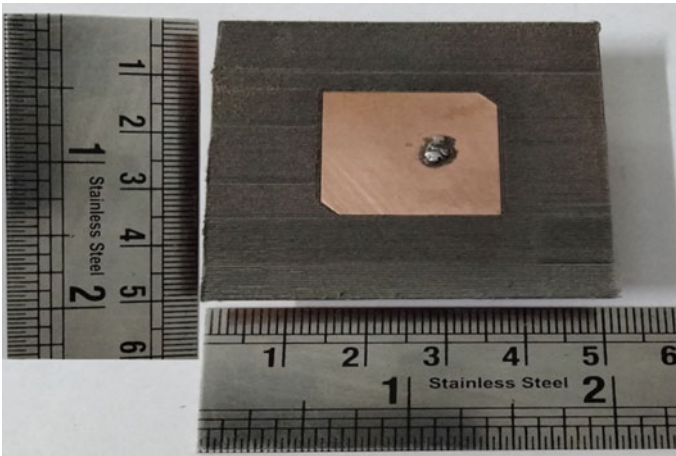


Fig. 2 Photograph of the suggested model

Table 1 Comparison of conventional single-feed circular polarization antennas

Reference No.	Axial ratio bandwidth (MHz)	Gain (dB)	10 dB Impedance bandwidth (%)
[2]	15	5.15	2%
[4]	18	4.4	-
[8]	21	5.8	2.37%
Proposed model	50	6.13	2.45%

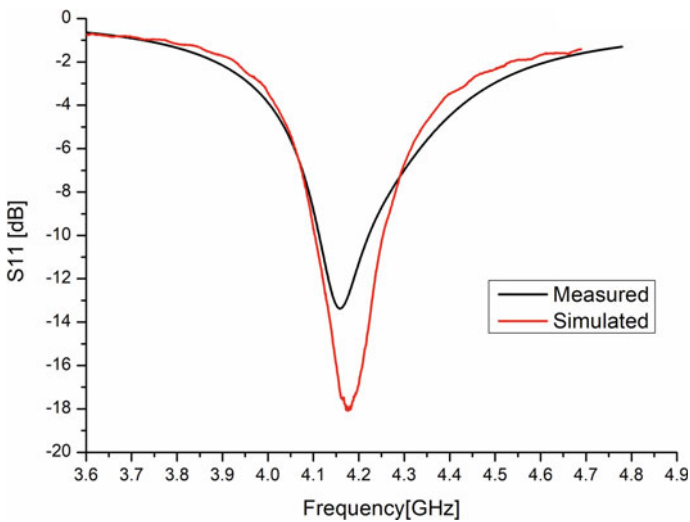


Fig. 3 Return loss of suggested model

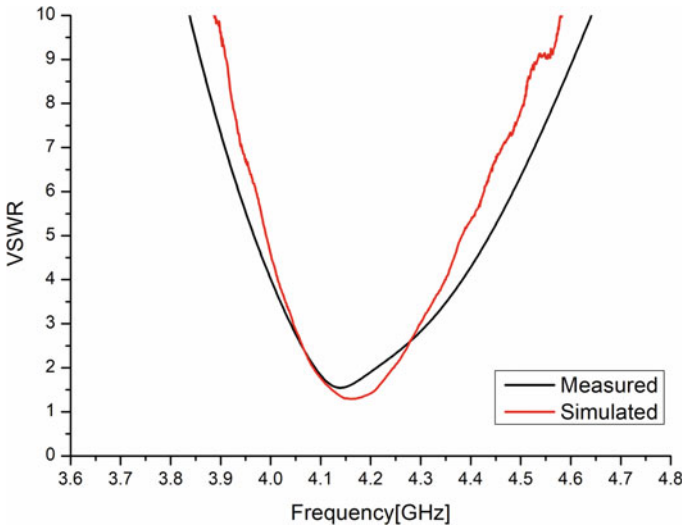


Fig. 4 VSWR of suggested model

and the simulated results are found to be 4.14–4.25 GHz (2.62%), and $VSWR \leq 2$ is observed which is shown in Fig. 4. Because of effects related to the cable, manufacturing imperfection and SMA connector, minor variations between the measured and simulated results are found. Comparisons for measured and simulated values of suggested structure are given in Table 2. The surface current distributions are shown in Fig. 5.

The pattern of radiation of the structure is computed at the centre frequency of 4.19 GHz in an anechoic chamber. The overall patterns of radiation on horizontal surface and vertical surface are computed using standard linearly polarized horn. Figure 6 shows patterns of radiation that are simulated and computed at 4.19 GHz, which shows excellent CP. The simulated and measured gains appear to be 6.28 and 6.13 dB for the band, respectively. The slightest axial ratio coinciding with the resonant frequency in the desired band of operation is illustrated through simulated axial ratio (shown in Fig. 7). The 3 dB AR bandwidth of 50 MHz (1.19%) can be observed in desired frequency band.

Table 2 Comparison for simulated and measured values of the suggested model at resonant frequency 4.19 GHz

Proposed antenna	Simulated	Measured
Return loss	−18.9 dB	−13.3 dB
Gain	6.28 dB	6.13 dB
Bandwidth	110 MHz	103 MHz
VSWR	1.32	1.48
Axial ratio	0.51 dB	1.24 dB

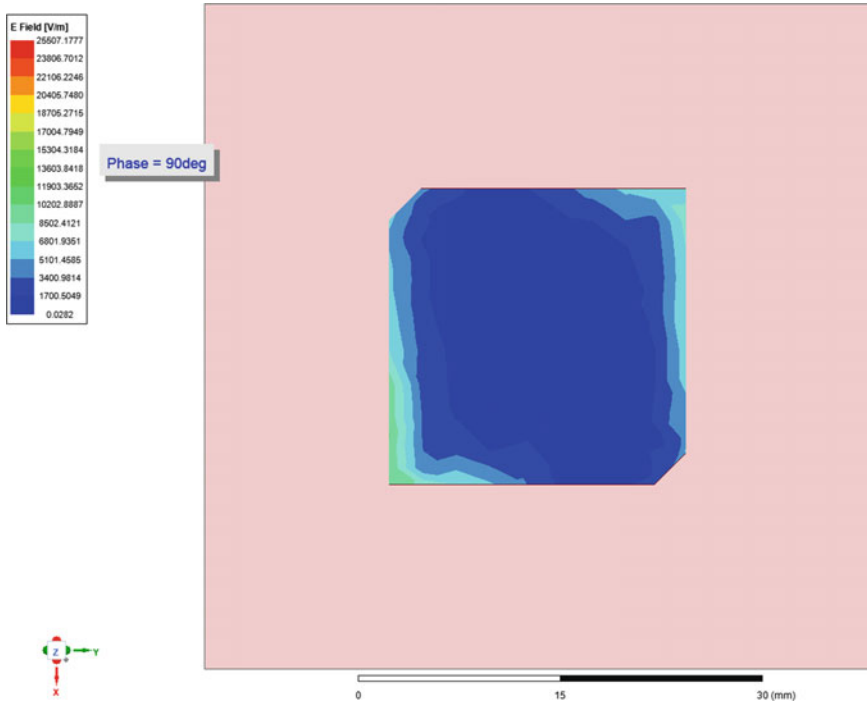


Fig. 5 Surface current distribution of suggested model

4 Conclusion

Designing of a circularly polarized patch antenna is performed successfully for the applications of C-band satellite. With a single patch and utilizing a substrate which has considerably thick low-dielectric constant, high gain and increased bandwidth can be produced. Diagonal corners of square patch are truncated to achieve circularly polarization (CP). The outcomes of the suggested antenna that are measured depict that besides reducing the size of the antenna, this structure also gives a wide operating bandwidth and excellent impedance matching over the desired band. Radiation patterns that are near omni-directional with adequate performance in terms of efficiency of the antenna and gain are exhibited by this antenna structure. On this account, the suggested antenna structure is apt for the current wireless communication applications.

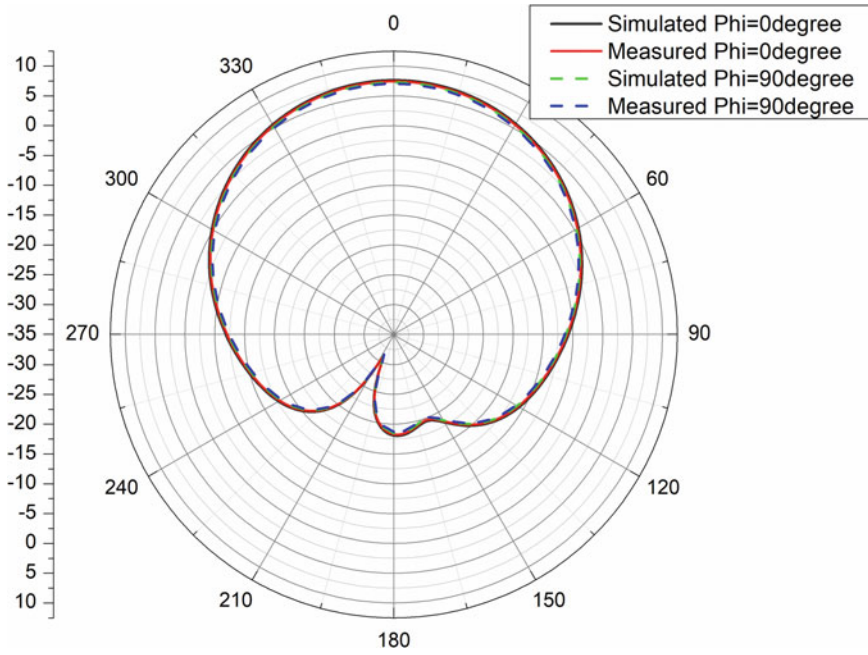


Fig. 6 Radiation pattern of suggested model

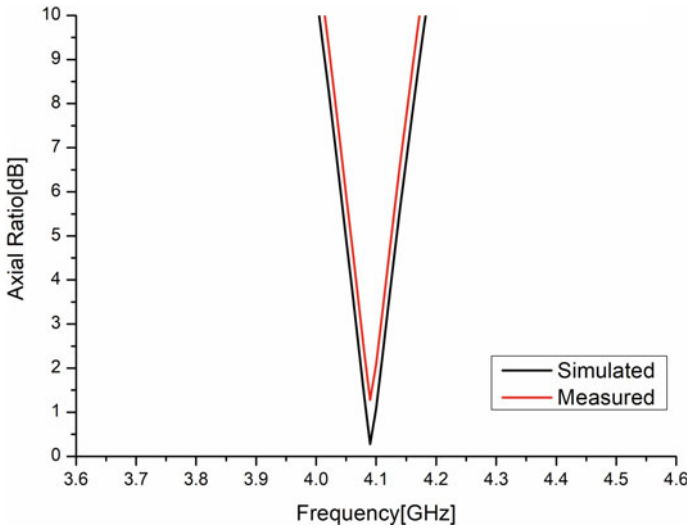


Fig. 7 Axial ratio of suggested model

Acknowledgements This work has been reinforced by the Science and Engineering Research Board (SERB), New Delhi, India (Grant No.: EEQ/2017/000118).

References

1. Falade OP, Rehman MU, Gao Y, Chen X, Parini CG (2012) Single feed stacked patch circular polarized antenna for triple band GPS receivers. *IEEE Trans Antennas Propag* 60(10):4479–4484
2. Yasin T, Baktur R (2013) Circularly polarized meshed patch antenna for small satellite application. *IEEE Antennas Wireless Propag Lett* 12:1057–1060
3. Pokuls R, Uher J, Pozar DM (1998) Dual-frequency and dual-polarization microstrip antennas for SAR applications. *IEEE Trans Antennas Propag* 46(9)
4. Yang Y-H, Guo J-L, Sun B-H, Huang Y-H (2016) Dual-band slot helix antenna for global positioning satellite applications. *IEEE Trans Antennas Propag* 64(12)
5. Di Carlo C, Di Donato L, Mauro G, La Rosa R, Livreri P, Sorbello G (2018) A circularly polarized wideband high gain patch antenna for wireless power transfer. *Microw Opt Technol Lett* 60(3):620–625
6. Iwasaki H (1996) A circularly polarized small size microstrip antenna with cross slot. *IEEE Trans Antennas Propag* 44(10):1399–1402
7. Wen-Shyang C, Chum-Kum K-L, Wong (2001) Novel compact circularly polarized square microstrip antenna. *IEEE Trans Antennas Propag* 49(3):340–342
8. Tong K-F, Wong T-P (2007) Circularly polarized U-slot antenna. *IEEE Trans Antennas Propag* 55(8):2382–2385
9. Adrian A, Schaubert DH (1987) Dual aperture coupled microstrip antenna for dual or circular polarization. *Electron Lett* 23:1226–1228
10. Tsao CH, Hwang YM, Killberg F, Dietrich F (1988) Aperture coupled patch antennas with wide-bandwidth and dual polarization capabilities. In: *IEEE antennas propagation symposium digestive*, syracuse, NY, pp 936–39
11. Pozar DM (1990) *Microwave engineering*. Addison-Wesley, Reading, MA
12. Squadrito P, Livreri P, Di Donato L, Squadrito C, Sorbello G (2019) A telemetry, tracking, and command antennas system for small-satellite applications. *Electronics* 8(6), Art. no. 689

An Integrated Methodology of TsF-KNN-Based Automated Data Classification and Security for Mobile Cloud Computing



P. Rajendra Prasad, V. Rupa, and K. Helini

Abstract In present days, most of the communication systems need the cloud technology. The data is transferred between the number of devices, so there is a chance of threats in the transformation of data. This can be prevented by using the data protection techniques. The security of the communication is required, and personal data can take more interest on this security of big data mobility. The present systems which provide the security are not having that much of efficiency because of its data determining techniques. For efficient data management, machine learning (ML) is used by the big data mobility. In a document public data and secret data, prediction is more complicated even by using some existed machine learning algorithms. Therefore, an integrated methodology-based automated data classification and security for mobile cloud computing of Training dataset Filtration Key Nearest Neighbor (TsF-KNN) classifier is introduced in this paper. This classification secures the mobile big data training datasets by using the integrated methodology with TsF-KNN classifier and Hadoop Distributed File System (HDFS). This process gives the best security in confidentiality level of the records. So the proposed model improves the security of the cloud system data mobility.

Keywords TsF-KNN · HDFS · Machine learning · Data security

1 Introduction

The last passing years, in the business world and in the information technology, cloud computing evolved as a revolution in the communication because it has some unique

P. Rajendra Prasad (✉) · V. Rupa · K. Helini
Vignan's Institute of Management and Technology for Women, Kondapur, India
e-mail: rajipe@vmtw.in

V. Rupa
e-mail: rupa@vmtw.in

K. Helini
e-mail: helini@vmtw.in

features such as low cost, resilient computing, rapid elasticity, service availability, ubiquity and massive scale, etc. The service is adopted by the cloud but not owned it; this is the main scheme of the cloud. The service of cloud environment is provided by virtual world [1]. Third party can control and manage the services of cloud computing. Cloud is a heterogeneous and open environment, so the data which is shared by the users has no command on it which leads to attacking of threats in the communication [2]. One of the artificial intelligence (AI) applications is machine learning, in which the systems can improve their experience automatically itself, not by depending on any externally assigned programs [3]. Computer program development is focused by the machine learning which can help in learning the data itself. In machine learning, data mining is one of the important applications. By considering some of the predictive features, algorithms of machine learning develop each instance in the dataset [4]. Hadoop Distributed File System (HDFS) is one of the service tools which are offered by the analysis of big data to huge amount of data storing, managing, human estimation risk decrement, and supports to speed up the automated decisions [5]. Different types of big data such as unstructured, semi-structured, and structured are managed by the HDFS. So it is most used dataset tool which supports the scalability, reliability, parallel processing, distributed architecture systems, and redundancy [6].

During data exchange or transmission, attacking of threats in the system. These threats are to be reduced to improve the security in the cloud environment data mobility systems which are provided in this paper. Especially in the transition of critical and sensitive data between the nodes of cloud systems, the security and privacy of big data are presented in this paper. The integrated process of big data is achieved by using TsF-KNN machine learning algorithm along with the HDFS system. The TsF-KNN algorithm is used to train the big datasets, and then, processed data is applied to the HDFS system to classify the huge amount of data. This model gives the best security to the confidentiality level of the records into two types as public and confidential.

2 Types of Cloud and Its Data Security Aspects

2.1 Types of Cloud

Each provider is having different capabilities and requirements to access the data. In that, some are fascinated to give high reliability and security by comparing others. Based on the problems of several service providers, the clouds are categorized as three types [7].

Public clouds: In which cloud service provider provides the resources to general public is commonly named as public cloud. For number of users, the infrastructure of cloud provides the service [8]. So this complex service is managed by the third party. But many companies have been working under this cloud environment because of its resources which serves the number of users. Service provider can manage the

responsibilities of the cloud. This cloud has some features such as no investment in the starting stage and no risks of shifting the infrastructure [9], whereas some drawback with this cloud is no restriction for access, so the system has to face the authentication issues. In this public cloud, the authorization and authentication techniques are not applicable because of its free access so the security problems are raised in this situation.

User Private Clouds: User private clouds are also called as “internal clouds.” The private organizations are operated by this user private cloud. For the specific applications, user private cloud is designed whereas public cloud is designed for the public in general applications [10]. The drawback of public cloud is overcome by this user private cloud in which high reliability, performance, and security are obtained. The public cloud is not appropriate for all environments of communications; in that case, this user private cloud is adopted by the service provider. This user private cloud architecture is too expensive than the architecture of public cloud so that it beats this advantages.

Hybrid Clouds: Two or more clouds are deployed to form this hybrid clouds. These clouds are not effected by each other but the transmission of data can happen between them [11]. In hybrid cloud, there is a requirement of management team to fulfill the requirements from the users and goals are provided by the service providers. This hybrid cloud is more flexible model to implement. The infrastructure is different for both public cloud and private cloud which are going to merge and gives the hybrid cloud [12].

2.2 *Cloud Data Security Aspects*

The three parameters influence the security that is integrity, availability, and confidentiality, in the information system such as software system, cloud network, and computer network. So the security of the system is obtained by this parameters. It is commonly named as a triad of CIA which stands for the confidentiality, integrity, and availability.

A. Confidentiality: From unauthorized user, the data protection is called as the confidentiality. The confidential information is transferred to the specified user. This confidential data is changed from one to another. The authorized user can get the exact information from the service provider. This confidentiality of the data depends on the impact and data type [13].

B. Integrity: Either the data is stored or it can be transferred from one place to another place depends on the integrity of the system which is more about the trustworthiness. If, by the unauthorized user, the data or information is damaged or changed, then there is a loss of the data integrity. In that case, the actual information is not received by the user exactly [14].

C. Availability: When there is a requirement, the data is accessed from the authorized entity or person which is called as availability of information. According to

its importance, the non-availability of the information of particular system changes [15].

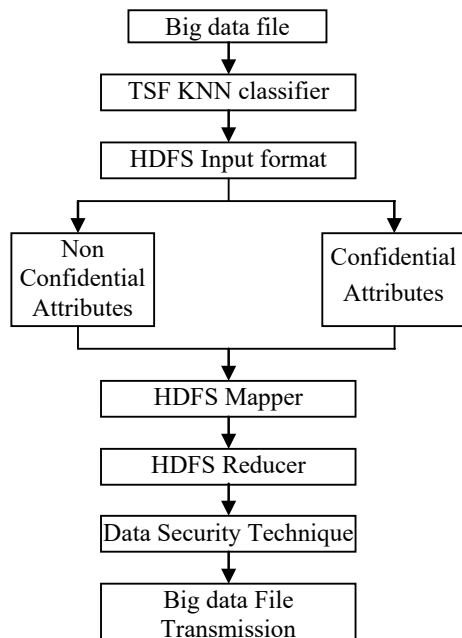
3 Integrated Methodology of TsF-KNN Based Data Classification and Security

In the cloud environment-based systems, the security is achieved by using the integrated method which is containing the security and classifies the files as two techniques of data mobility. The framework of TsF-KNN classifier-based integrated cloud data security is described in the Fig. 1. The following sections give the clear idea about the security and classification of the big data file.

3.1 Big Data File

Based on the test file properties and metadata, the file name is predicted by the first document properties and then the determination of the nearest sub-training datasets. The document of data may be mixed in nature, or it will be in multiple categories. Then, the data confidentiality is predicted as either it is the category of confidential

Fig. 1 Framework of TsF-KNN classifier-based integrated cloud data security methodology



or non-confidential. According to security of the data, importance and quality are changed for each attribute.

3.2 TsF-KNN Classifier

The workload of the training data set increased by reduced classifier by using new filtration system in TsF-KNN algorithm. Another name of this system is “bi-gram with dice coefficient” applied before the KNN classifier. In this step, classify data accuracy is improved, and at the testing phase, the KNN complexity is reduced. In this TsF-KNN algorithm, the integration of bi-gram model with the KNN is occurred which makes the proficiency in classification and improved accuracy in the KNN algorithm. By using this filtration process, the repetitions are reduced in the algorithm and computational effort is reduced. From datasets created by researchers or from the MobiPerf Open Google Mobile Data Repository, the required training samples of mobile datasets are collected.

3.3 HDFS Input Formatter

The data in files is existed in various types like pdf, doc, txt, csv, xml, sql, xls, db, log, audio, image, video, etc. [16]. By using the HDFS Customized Input Format (HCIF), the splitting of the converted big data is processed as each of size as 128 MB smaller input partitions. The main object of this proposed classification is the conversion of the files pdf, doc, txt, csv, xml, sql, xls, db, log, audio, image, and video into text files and splitting as smaller parts by using HDFS input formatter. Each splitting partition is having the size of 128 MB; for the input specification task, input formatter is validated. The specific size of spitted data is not exceeding the available memory, so to make memory free, no additional techniques are required. For the input specification task, HDFS input formatter validates and input data files are going to split according to the specific size of each as 128 MB. Input formatter is the input specification [16]. Confirmed task does not exceed the available memory, so to make memory free, no additional techniques are required.

3.4 Big Data Classification

Depending on the complexity and data sensitivity, the classification of big data can be processed based on degrees of protection, priorities, and its needs. The classification technique in this paper, the big data, is categorized into two types as public or confidential based on the risk management level which is explained as below:

- Based on values of risk assessment metrics, RIL represent that risk impact level may work.
- The extended attribute is represented by the MAV (Metadata Attribute Values) which is computed by using the following equation:

$$\text{MAV} = \begin{cases} 0, & 0 \leq \text{RIL} \leq 1 \\ 1, & \text{RIL} > 1 \end{cases}$$

If the risk impact value is between low and very high (1–5) [16], then the MAV returns True (1: confidential) and the risk impact value is not significant or insignificant (0–1), then it gives the False (0: public). To smooth the progress of classification processes, in the file metadata MAV is inserted. There is mapping process that occurred to the every small category which is spitted in mapper. The files are described in the following as:

- **Confidential Data:** Very high sensitive data is represented by the confidential data, and that can be transferred to the authorized users only. The specific data can be operated by this authorized user, and it contains the information about that particular company or organization such as financial details and health information of patient. Potential risks on files are eliminated in the sensitive information by the implementation of confidential metadata attributes.
- **Public Data:** The information in the public data is viewed by anyone without any restrictions. The data can also be accessed by the unauthorized user so the information in this public data is unprotected.

3.5 *HDFS Mapper*

Based on the predefined policy, HDFS Mapper is assigned by the every partition so it can read the contents in that which is used to classify confidential or public data. On each partition, the mapper works.

3.6 *HDFS Reducer*

The output of the mappers is given to the HDFS Reducer as its inputs. The output of this reducer gives single value as 0 for public data and 1 for the confidential data.

3.7 *Big Data Security Technique*

Depending on the classification of data file, among the several nodes of the cloud, procedures of security are applied to the mobile big data. If the classification results as public, then there is no requirement of security actions, and if the classification gives the result as confidential, then the security actions are processed as follows:

1. In the cloud, all the shared credentials are secured with the sender and receiver. Then, the metadata is sent to the sender, and by shareable access, data between user and sender/recipient in cloud is encrypted.
2. The receiving data nodes receive its encrypted data by using a random access key, data blocks IDs, and addresses from the sender.
3. For security reasons, it shares all keys to access encrypted blocks with all its nodes.
4. By using the encrypted block access key, the receiver triggered the request for move data and save transmitter data nodes.
5. Data node is decrypted for authentication after receiving the request from the sender.
6. When the sender sends the data packets, the receiver receives it after it is confirmed with acknowledgment process. The process of transmitting data packets is repeatedly done by the sender until the receiving of delivery confirmation; otherwise, the data admin in the sender part is get informed if there is exceed of failed trails to allowed limit.
7. The receiving node checks with its hash value after receiving the data packets from the source.
8. If the conformation of the data packet hashes value, then encrypted acknowledgment is send to the sender data node by the receiver. Number of copies of same data packets are received by the receiver data node, if there is a missing in the acknowledgment. In this situation, the recurring data packets are ignored.
9. The receiver receives data when the sender receives the acknowledgment and then keeping or deleting the data after the successful completion of data transferring.

4 Results

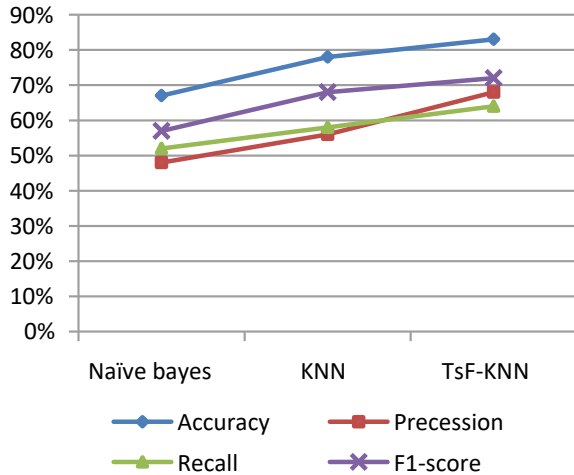
The 5 different file types such as csv, sql, log, and xls that are used in this paper are classified into public/secured using TsF-KNN and to provide security for the classified data. The analysis performance of algorithms of TsF-KNN with traditional KNN and Naïve Bayes by taking the 5 datasets is described in Table 1 (Fig. 2).

The average values are obtained in the table. The algorithm of TsF-KNN has the rate of accuracy as 0.83 (83%), rate of precision is 0.68, rate of $F1$ -Score is 0.72 (72%), and recall rate is 0.64. The KNN has the second highest classification performance. According to the table, the KNN algorithm is having the low accuracy

Table 1 Performance comparison between Naïve Bayes, KNN, and TsF-KNN Classifiers

Classifier	Naive Bayes	KNN	TsF-KNN
Accuracy	0.67	0.78	0.83
Precision	0.48	0.56	0.68
Recall	0.52	0.58	0.64
F1-Score	0.57	0.68	0.72

Fig. 2 Performance comparison of different classifiers



than the TsF-KNN and having higher accuracy while it comparing with the Naïve Bayes (NB) algorithm. *F1-Score* rate is maximum at the algorithm of TsF-KNN as 0.72 (72%). The average *F1-Score* rates of NB algorithm and traditional KNN algorithms are 0.57 (57%) and 0.68 (68%), respectively. The minimum *F1-Score* rate is obtained at the Naïve Bayes. The files of TsF-KNN algorithm data can be classified into two types according to the *F1-Score* results either it is confidential or non-confidential data. The efficiency of the TsF-KNN algorithm is high by comparing it with the NB algorithm and traditional KNN algorithm.

After the user authentication, the transmitting of big data can be processed between the nodes of cloud. By integrating a public key with the user private key, the authentication of the user at the receiver and sender nodes is carried out. The comparative experimental results of presented secured system with the secured HDFS and non-secured Hadoop base line in terms of secured data transmission throughputs are taken. The secured HDFS method side effects on transmission throughput of big data can be studied, and secure data transmission bandwidth is defined as the average amount of data or the number of bits transmitted from the source cloud to the destination cloud and is divided with the SDDT (Secure Data transmission Response Time). This response time is measured in the form of megabits per second.

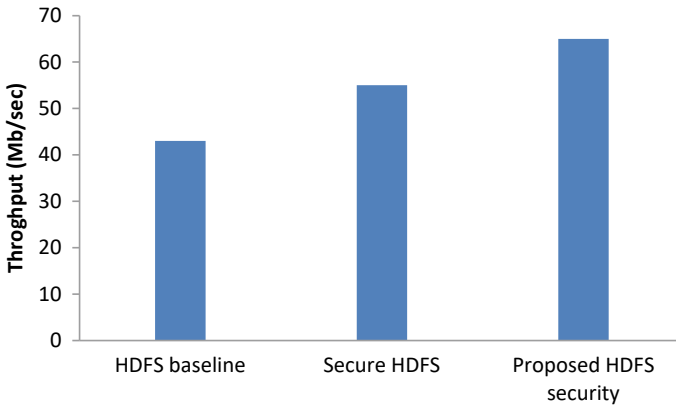


Fig. 3 Comparative analysis of SDTT

HDFS security method throughput is presented in Fig. 3. So it can be concluded that increasing the file size gives the decrement in the transmission throughput of inter-cloud data. Throughput shortage is happened by all the secured HDFS methods.

5 Conclusion

In this paper, using machine learning concepts, we have classified mobile learning datasets with cloud storage using the TsF-KNN algorithm and HDFS big data analysis model representing computations that ensure the integrity and confidentiality of categorization of critical data is guaranteed. In this TsF-KNN algorithm, the bi-gram model is integrated with KNN to improve the classification ability and increase the accuracy of the KNN algorithm. This filtering process reduces iterations in the algorithm and reduces computational effort. The data attributes are classified into two classes as secret and non-secret by the KNN algorithm. With this classification and security of big data, cloud systems achieve a high level of data mobility and avoid threats and risks. HDFS Mapper is assigned by each partition so that it can read the content, which is used to classify data, whether secret or public. In the current model, cloud performance is based on the security we provide for identified files and additional costs should be reduced for this process. The performance of the presented model is shown by performing the simulation results.

References

1. Buyya R, Gill SS (2020) Failure management for reliable cloud computing: a taxonomy, model, and future directions. *Comput Sci Eng* 22(3)

2. Xia S, Li Y, Liu Q, Cao B, Zheng M (2019) Lyapunov optimization based trade-off policy for mobile cloud offloading in heterogeneous wireless networks. *IEEE Trans Cloud Comput*
3. Hui P, Chemouil P, Li Y, Kellerer W, Tao D, Stadler R, Zhang Y, Wen Y (2019) Special issue on artificial intelligence and machine learning for networking and communications. *IEEE J Selected Areas Commun* 37(6)
4. Kong L, Xin Y, Chen Y, Liu Z, Wang C, Zhu H, Li Y, Hou H, Gao M (2018) Machine learning and deep learning methods for cybersecurity. *IEEE Access* 6
5. Selvamuthukumar S, Suganya S (2018) Hadoop distributed file system security—a review. In: *International conference on current trends towards converging technologies (ICCTCT)*
6. Tianfield H, Win TY, Mair Q (2018) Big data based security analytics for protecting virtualized infrastructures in cloud computing. *IEEE Trans Big Data* 4(1)
7. Sharma SJ, Prajapati AG, Badgujar VS (2018) All about cloud: a systematic survey. In: *International conference on smart city and emerging technology*
8. Gehrman C, Paladi N, Michalas A (2017) Providing user security guarantees in public infrastructure clouds. *IEEE Trans Cloud Comput* 5(3)
9. Hong P, Xue K (2014) A dynamic secure group sharing framework in public cloud computing. *IEEE Trans Cloud Comput*
10. Kao CH, Lu HT, Lee Yh, Wu PH (2014) Towards a hosted private cloud storage solution for application service provider. In: *Proceedings of 2014 international conference on cloud computing and internet of things*
11. Crişan-Vida M, Chioreanu R-C, Stoicu-Tivadar V, Stoicu-Tivadar L (2014) Implementing and securing a hybrid cloud for a healthcare information system. In: *11th International symposium on electronics and telecommunications (ISETC)*
12. Da Silva AF, Tronco ML, Valencio CR, Cansian AM, Guimaraes DL (2013) GBD IAAS manager: a tool for managing infrastructure as-a-service for private and hybrid clouds. In: *2013 International conference on parallel and distributed computing*
13. Xiao Y, Xiao Z (2013) Security and privacy in cloud computing. *IEEE Comm Surv Tutor* 15(2)
14. Foresti S, Samarati P, Capitani di Vimercati SD, Paraboschi S, Jajodia S (2013) Integrity for join queries in the cloud. *IEEE Trans Cloud Comput* 1(2)
15. Tzeng W-G, Lin H-Y (2012) A secure erasure code-based cloud storage system with secure data forwarding. *IEEE Trans Parallel Distrib Syst* 23(6)

Cascaded H-Bridge Multilevel Inverter for PV Applications



P. Srujay, Sd. Abeeunnisa, N. Prasad, K. Hanu Vamshi, and M. Srinivas

Abstract In present scenario, photovoltaic power systems are getting extensive with the rapid magnification in the energy consumption and the care for the environmental contamination. Present PV systems are ranging from few kilowatts to several megawatts; therefore, grid integration of PV system is getting prominence in many countries. Multilevel inverter acts as a promising solution for grid connected PV systems due to their substitutable and reduced voltage stress over the switches. Out of different structures, cascaded H-bridge multilevel inverter is highly appropriate for PV approach since every PV panel can act as an individual DC source for every cascaded H-bridge module. In this paper, a comparative analysis of four different levels of multilevel inverter is presented. Control scheme designed on sinusoidal pulse width modulation (SPWM) is used due to its ease of implementation. As the number of levels increases, results in reduced total harmonic distortion (THD) and the output will be nearly sinusoidal.

Keywords Multilevel inverters · Sinusoidal pulse width modulation · Total harmonic distortion

1 Introduction

Multilevel inverters are getting popular because they can produce highly sinusoidal voltage at high power and medium voltage applications by adding many low voltage power devices as input. With the use of multilevel inverters, filters can be reduced or eliminated. There are different types of multilevel inverters; out of these different types, we use cascaded H-bridge multilevel inverter, and it is more suitable for PV applications.

P. Srujay (✉) · Sd. Abeeunnisa · N. Prasad · K. Hanu Vamshi · M. Srinivas
EEE Department, Kakatiya Institute of Technology and Science, Warangal, India
e-mail: srujay2000@gmail.com

1.1 Multilevel Inverter

Inverter is a device, which is capable to provide required ‘alternative voltage’ level at the output using various lower-level ‘dc voltages’ as an input. These are used for high and medium voltage (V) applications. When compared to conventional type inverter, multilevel inverter has low total harmonic distortion (THD) value and gives sinusoidal output. Based on the source of input voltage and switching mechanism, they are 3 types: diode clamped, flying capacitors, and cascaded H-bridge.

Cascaded multilevel inverters are based on a sequence of single H-bridge connections with discrete direct current (‘DC’) sources. These direct current (‘DC’) sources may be any natural resource inclusive of sunlight or wind energy or anything. The major benefit of this kind of multilevel inverter is that it requires a lesser quantity of elements in comparison with other MLI. Cost of the inverter and weight of the inverter are much less than the ones of the other 2 inverters. The output waveform is closely sinusoidal.

1.2 Three-Level H-Bridge Multilevel Inverter

Firstly, consider the case of a 3-level inverter [1] as shown in Fig. 1. The full bridge itself is a 3-level H-bridge multilevel inverter. For the purpose to change the voltage (‘Vdc’) level in the H-bridge stage, the multilevel inverter switches on and switches off the other in the full bridge inverter. We consider Vdc as an input, and we will get an output of 3 levels (+Vdc, 0, -Vdc). Each module is added in cascade, adding

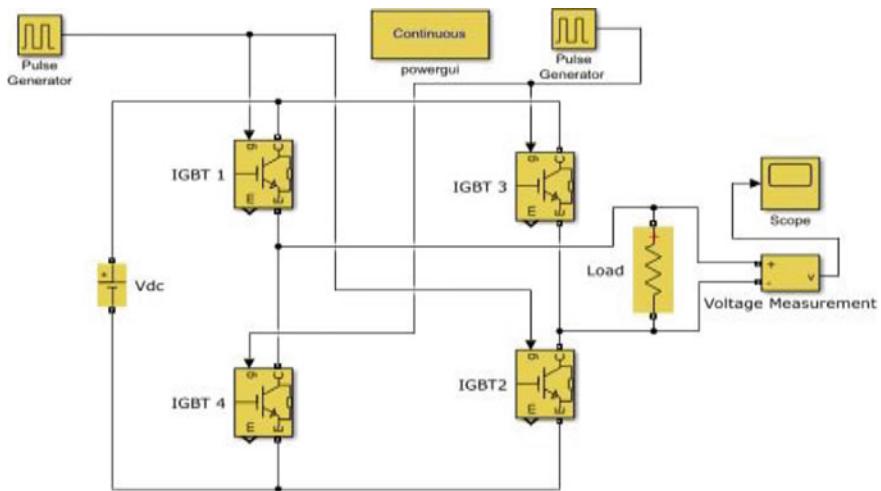


Fig. 1 3-Level circuit diagram

two voltage levels to the inverter. The output voltage waveforms and FFT analysis of three-level MLI can be viewed from Figs. 2 and 3.

Operation of three-level inverter can be explained below.

Mode: +V_{dc}: In this stage, switches 1 and 2 are turned ON and switches 3 and 4 are turned OFF.

Mode: Zero Voltage: When there is no flow of current in the circuit, we obtain the zero voltage.

Mode: -V_{dc}: In this stage, switches 3 and 4 are turned ON and switches 1 and 2 are turned OFF.

Mathematical Calculation:

- No. of Switches = $2*(n-1)$, where n = number of levels.
- Let Input Voltage = 100 v

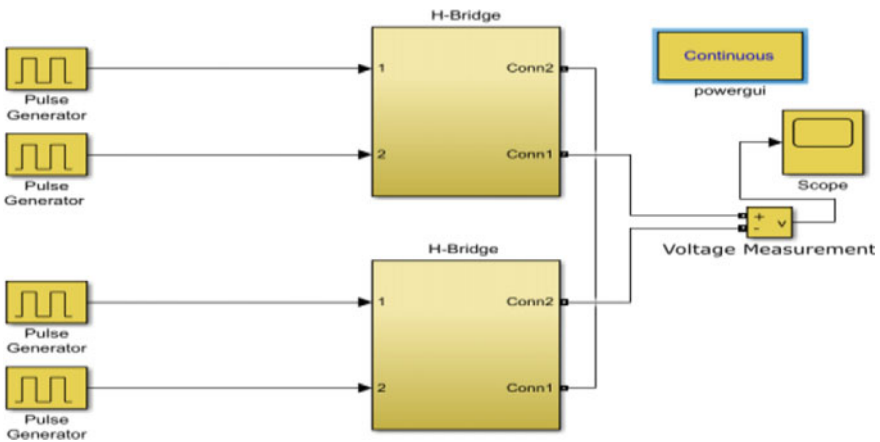


Fig. 2 3-Level output waveform

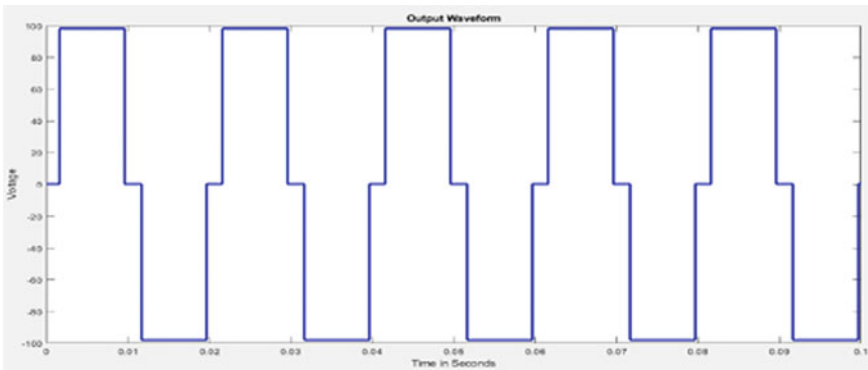


Fig. 3 3-Level FFT analysis

- Consider Load as Resistance (R) = 100 ohms
- For Pulse Generator: Pulse Amplitude = 1, Period $\Rightarrow F = 1/T \Rightarrow$ for $F = 50$ Hz $\Rightarrow T = 0.02$ s
- Pulse Width = 40
- Phase Delay for P1 = Consider $30^\circ \Rightarrow 360 = 0.02 \Rightarrow 30 = 1.6e-3$ s
- Phase Delay for P2 = $30 + 180^\circ \Rightarrow 210 \Rightarrow 0.01166$ s

1.3 Five-Level CHB-MLI

Figure 4 represents a 5-level inverter, which includes H-bridge cells related in series, which can be related through impartial voltage sources. Output of the two distinct stages is related in collection in order that the output voltage signal is the combination of separate outputs. We are going to use 2 voltage sources here, i.e., ($V = V_{dc} + V_{dc}$) which produce 5 levels of output like $2 V_{dc}$, V_{dc} , 0 , $-V_{dc}$, and $-2 V_{dc}$. Figure 5 represents output waveform, and Fig. 6 represents FFT analysis.

2 Sinusoidal Pulse Width Modulation

The input to a voltage source inverter is DC which is constant in magnitude. The basic role of a conventional inverter is to transfigure DC input with unceasing magnitude to alternating current ('AC') output having variable frequency and magnitude. The efficient method of doing this is by controlling width of pulses, known as pulse width modulation (PWM) control. There are several techniques of PWM. In this project, we have used sinusoidal pulse width modulation method. In 'SPWM' method, the width of constant amplitude output pulse from the inverter is modulated by frequently opening and closing the switches at high speed, for obtaining controlled output

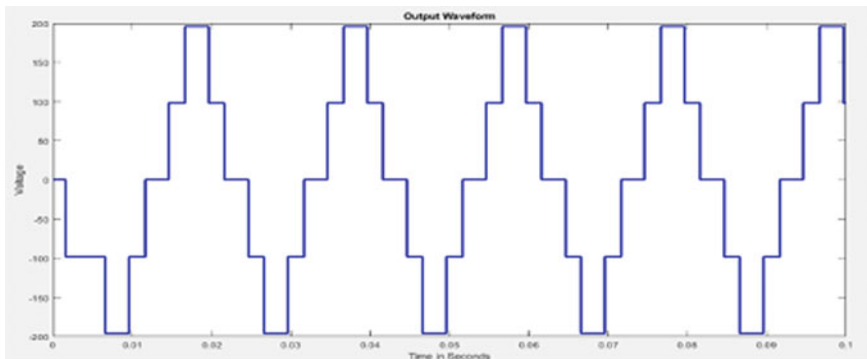


Fig. 4 5-Level circuit diagram

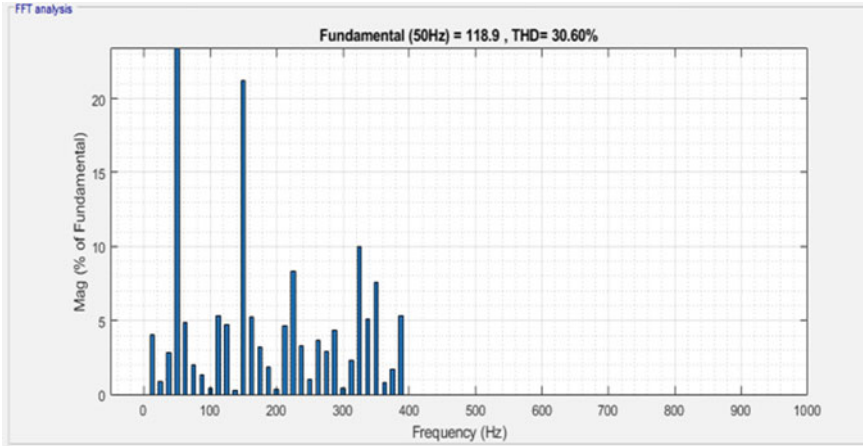


Fig. 5 5-Level output waveform

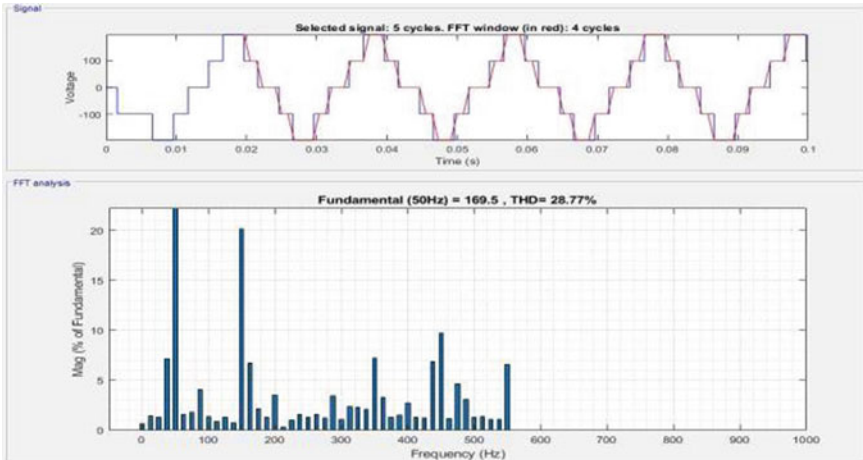


Fig. 6 5-Level FFT analysis

voltage and reduced harmonic content. We can use MOSFETs or IGBTs as switches because they have a higher switching frequency and lower switching power loss. The circuit for the control signal generation can be done using the following Figs. 7 and 8.

In this technique, the triggering pulses for the switches are produced by relating triangular waveform (carrier signal) having high frequency with a sinusoidal waveform (reference signal) of the specified frequency. A high switching frequency results in a far better sinusoidal output waveform and fewer THD. To get the desired output voltage and frequency, the amplitude of the reference signal is to be varied.

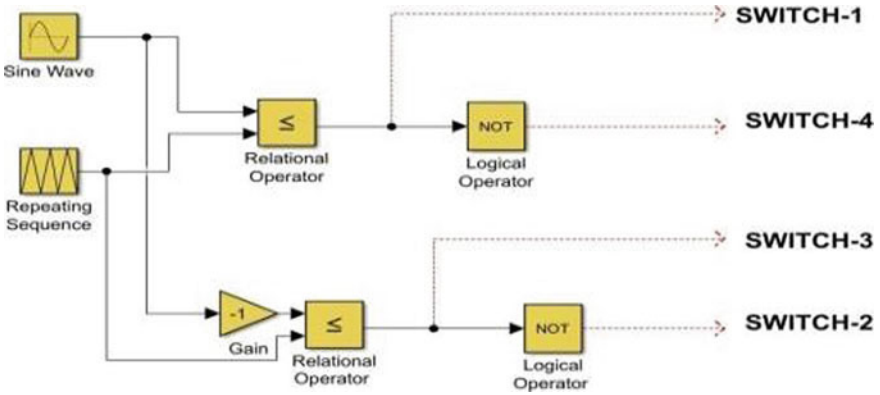


Fig. 7 Control signal generation

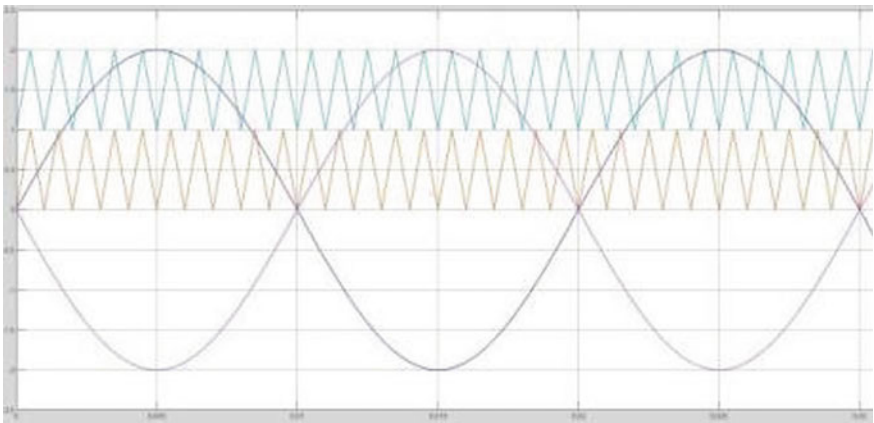


Fig. 8 Reference and carrier signal

For a five-level inverter, we want two triangular carrier signals of various magnitudes, and that we compare it with a low frequency wave with the help of a comparator. When the magnitude of reference signal is a smaller amount than the carrier signals, the output of the comparator is high; otherwise, it is low. The output pulses are generated from the comparator that are given to the gate terminals of switches inside H-bridge as shown in above figures.

3 Five-Level CHB-MLI Using SPWM

Simulation is done using the MATLAB. The simulation diagram for 5th-level inverter is shown in the Fig. 9. For the 5-level inverter, we need 8 switches. Here, we have used MOSFET as switching devices (Tables 1 and 2).

Operation of five-level CHB-MLI using SPWM is explained below.

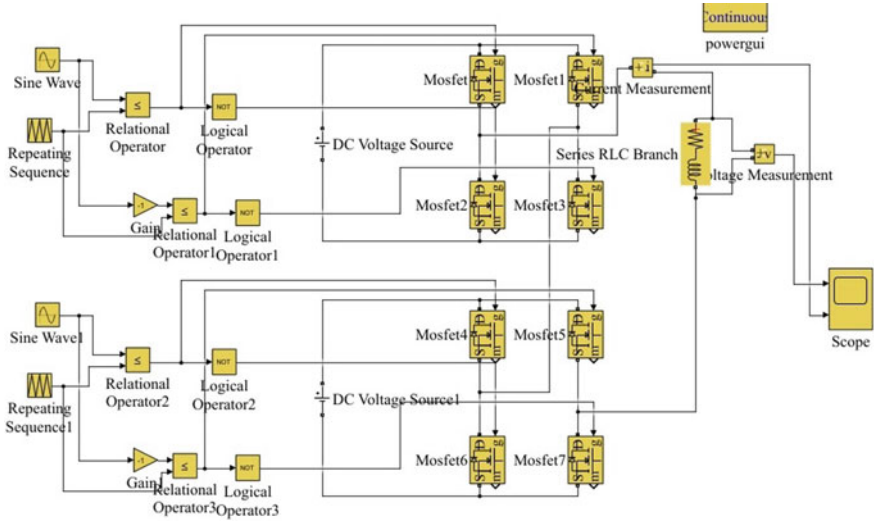


Fig. 9 5 levels with R-L load using SPWM

Table 1 Design parameters of 5-Level CHB-MLI

S. No.	Parameter	Five-level inverter
1	Input voltage (Vdc)	100 V
2	Load	$R = 100 \Omega, L = 100e-3H$
3	Carrier wave frequency	1000 Hz
4	Reference wave frequency	50 Hz
5	Input voltage (Vdc)	100 V

Table 2 Comparison of THD values

No. of levels	No. of switches required	% THD using conventional	% THD using SPWM Technique	
			R load	R-L load
Five level	8	28.77	26.95	27.03
Seven level	12	21.93	20.40	20.50
Nine level	16	20.32	18.07	18.17

Mode 1: +Vdc: In this mode of operation, switches 1, 2, 5, and 7 are ON and remaining switches are in OFF position.

Mode 2: +2 Vdc: In this mode of operation, switches 1, 2, 5, and 6 are ON and remaining switches are in OFF position.

Mode 3: In this mode of operation, switches 1, 3, 5, and 7 are ON and remaining switches are in OFF position.

Mode 4: -Vdc: In this mode of operation, switches 3, 4, 5, and 7 are ON and remaining switches are in OFF position.

Mode 5: -2Vdc: In this mode of operation, switches 3, 4, 7, and 8 are ON and remaining switches are in OFF position.

The output voltage waveforms and FFT analysis of five-level CHB-MLI using SPWM are represented in Figs. 10 and 11.

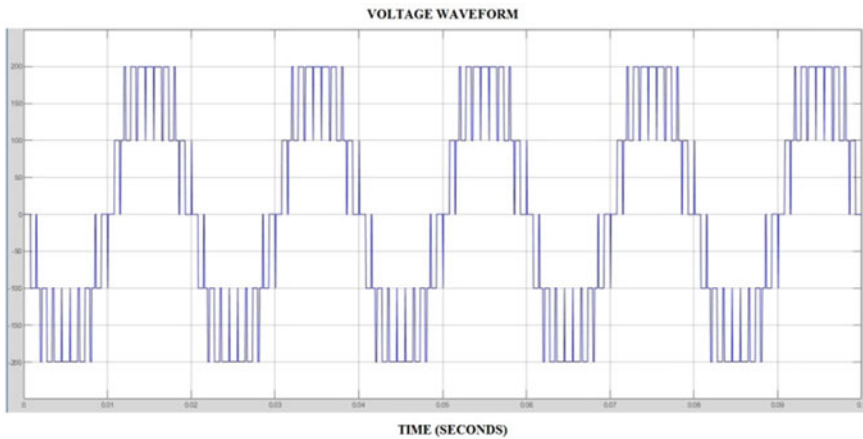


Fig. 10 5-level voltage waveform using SPWM

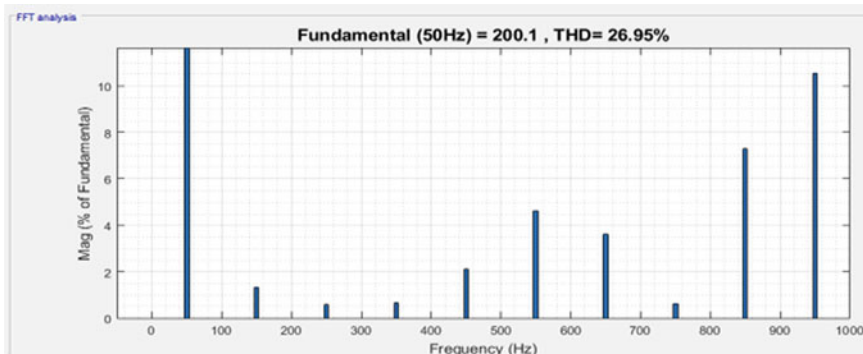


Fig. 11 5-level FFT analysis using SPWM

Simulation is done using the MATLAB. The simulation diagram for 7-level inverter is shown in the Fig. 12. For the 7-level inverter, we need 12 switches. Here, we have used MOSFET as switching devices. The output voltage waveforms and FFT analysis of seven-level CHB-MLI using SPWM are represented in Figs. 13 and 14.

Here, simulation is done using the MATLAB. The simulation diagram for 9-level inverter [2] is shown below. For the 9-level inverter, we need 16 switches. Here, we have used MOSFET as switching devices. Nine-level inverter is explained using Figs. 15, 16, and 17.

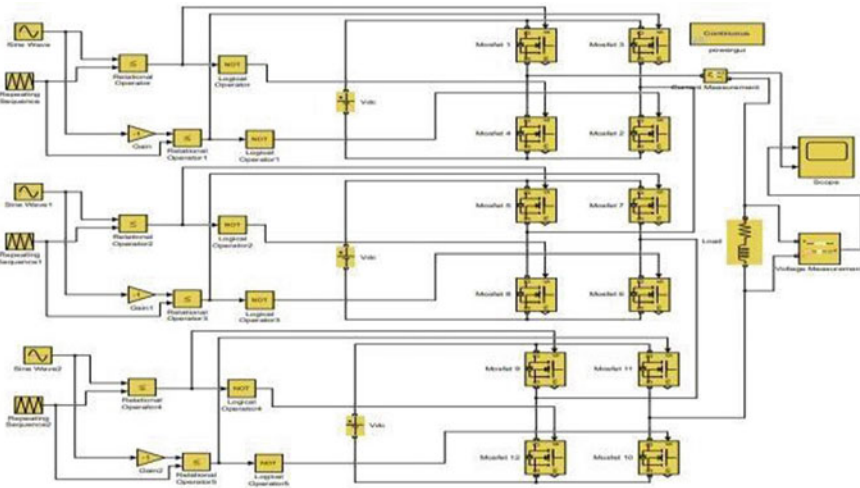


Fig. 12 7 levels with R-L load using SPWM

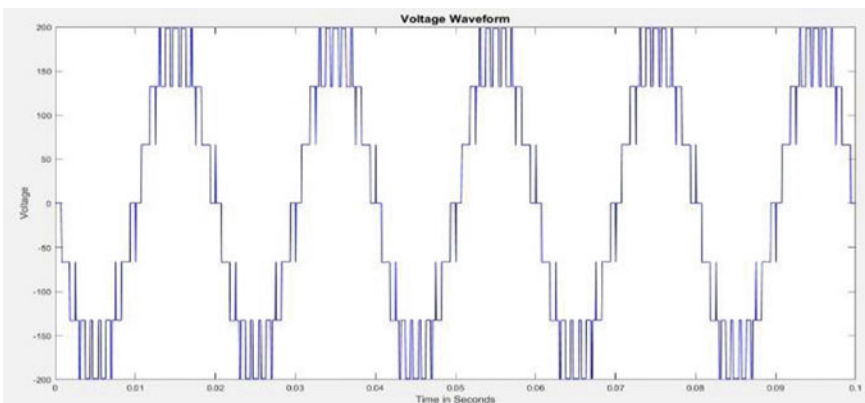


Fig. 13 7-level voltage output using SPWM

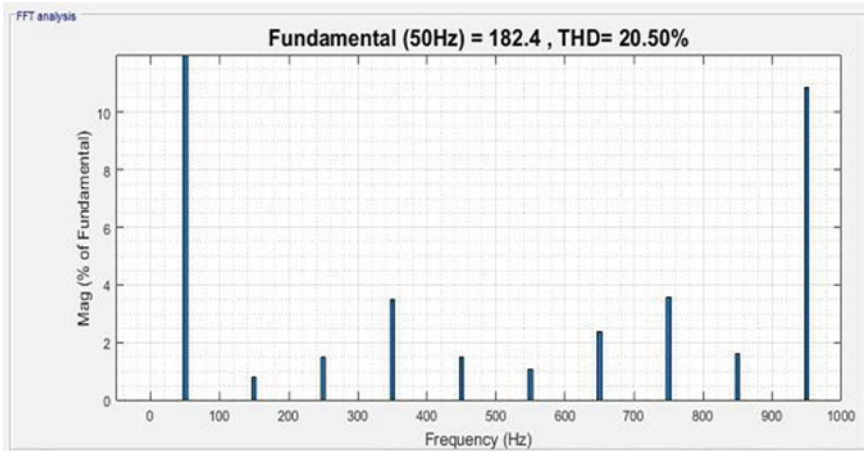


Fig. 14 7-level FFT analysis

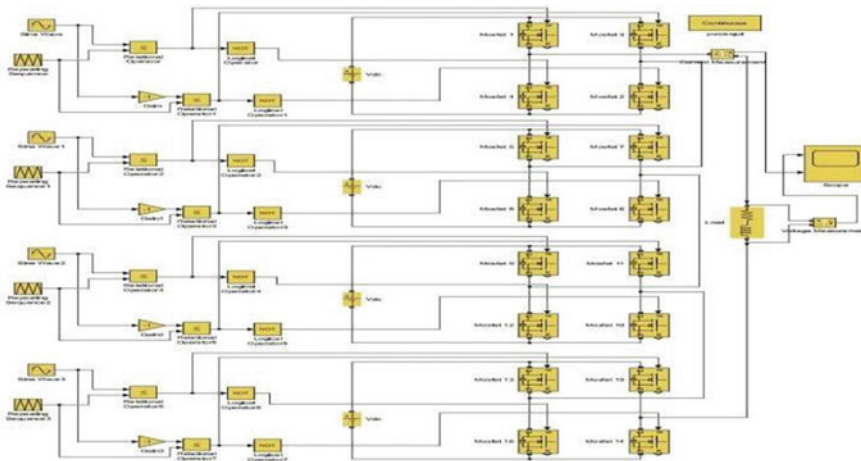


Fig. 15 9 levels with R-L load using SPWM

4 Comparison of THD

It can be observed that there is a great reduction in THD [3] values as compared to conventional inverters. The THD is obtained as '18.07' % for the nine-level inverter which is less than the five- and seven-level inverter. Therefore, here we observed that as the levels in output voltage are increasing, the total harmonic distortion (THD) is decreasing and the waveform is approaching to pure sinusoidal.

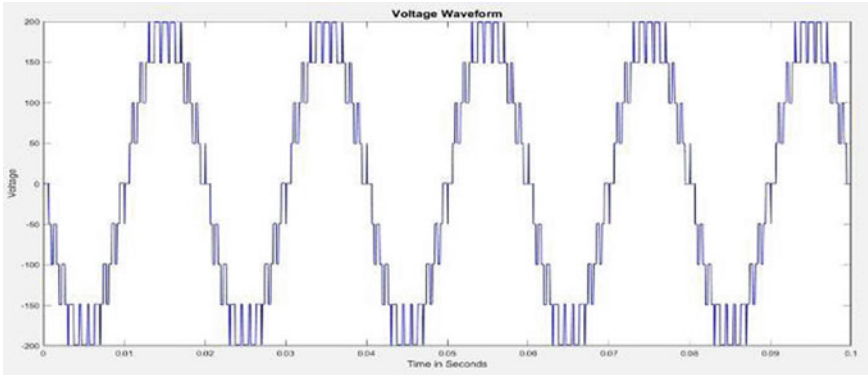


Fig. 16 9-level voltage waveform

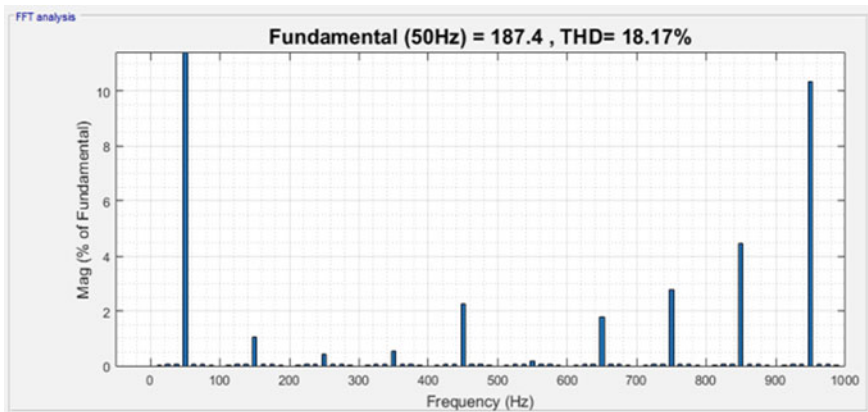


Fig. 17 9-level FFT analysis

5 Photo Voltaic Cell

Photo voltaics is the most famous method of using solar cells to generate electricity, using the photoelectric effect to convert solar energy into a stream of electrons. Solar panels generate 'direct current (dc)' from sunlight, which are used to operate equipment or charge batteries. Photovoltaic cells encompass dual or greater layers of semiconductors with one layer containing a positive charge and the other with a negative charge which is adjoining to every other. Sunlight, comprising of little parcels of energy named as photons (positive charge), strikes the solar cell, where it is either reflected or consumed. The photons are attracted by the negative charge particles of the photovoltaic (PV) panel, and the energy of the positive charge gets moved to negative charge in an iota of the panel. The expansion in energy, the negative charges get away from the external shell of the particle. The negative charge

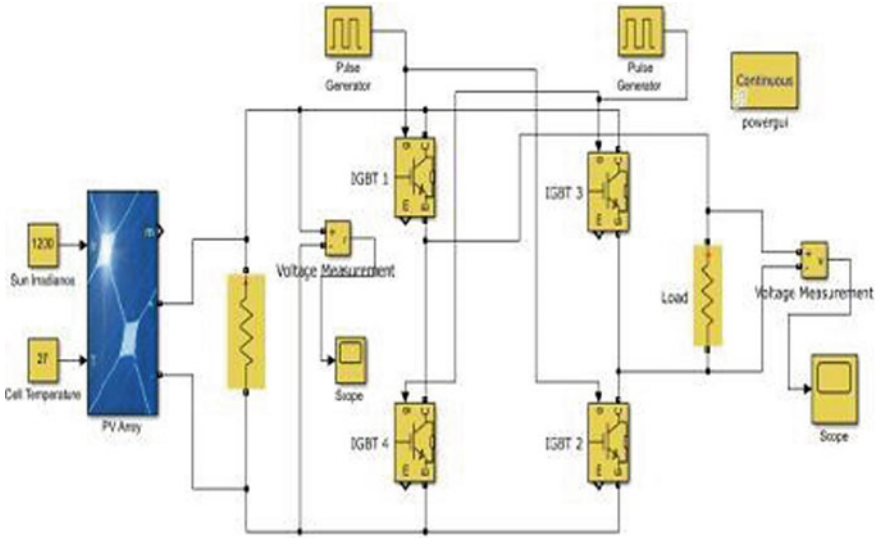


Fig. 18 3-level diagram using PV array

particles normally relocate to the positive charge particle making an expected contrast between the positive layer and the negative layer. At the point when the two layers are associated with an outside circuit, the electron courses through the circuit, making a current.

5.1 Simulation of MLI Using PV Panel

Simulation of 3-Level MLI using PV Array:

Figure 18 represents simulation circuit of 3-Level MLI using PV Array [4]. In this circuit, a PV Array is added for simulation and the specifications are mentioned in Table 3. Figure 19 gives the output waveforms of three-level inverter.

6 Conclusion

Multilevel inverters provide numerous advantages when compared with the two-level inverters, and these can be used to handle high power applications. In this project, the single-phase five-, seven-, and nine-level CHB-MLI is studied and analysis is done in terms of parameters like output voltage, current, and total harmonic distortion (THD). SPWM modulation technique is used for generation of switch pulses to the inverter.

Table 3 Solar module specifications

S.No	Parameter	Solar module
1	Module	1Soltech-1STH-215-P
2	Irradiance (w/m ²)	1200
3	Temperature	27 °C
4	No. of series connected modules	03
5	Open circuit voltage of each module	36.3 V
6	Output voltage	85 V

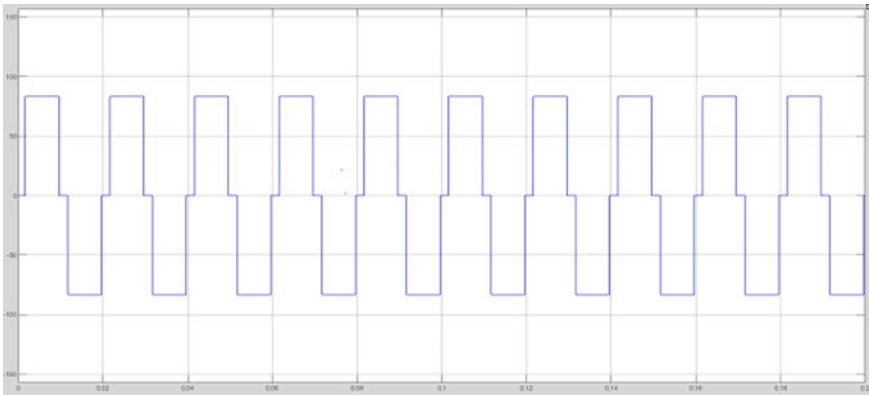


Fig. 19 Output waveform using PV array

From Table 2, we can analyze that as the level increases, we will give output almost sinusoidal wave form and reduction in THD from 27.03 to 18.17, which can be used for motor drive applications, variable speed control, and also for interfacing renewable energy resources such as the solar energy.

References

1. Rashid MH (2006) Power electronics: circuits, devices and applications. 3/E
2. Satheesh Kumar P, Natarajan SP, Nachiappan A, Shanthi B (2013) Performance evaluation of nine level modified CHB multilevel inverter for various PWM strategies. *Int J Modern Eng Res (IJMER)* 3(5):2758–2766
3. Yadav A, Kumar J (2013) Harmonic reduction in cascaded multilevel inverter. 2(2):147–149, ISSN:2277-3878
4. Daher S, Schmid J (2008) Multilevel inverter topologies for stand-alone PV systems. *IEEE Trans. Ind. Electron* 55–57

Dual-Band Circularly Polarized Pentagon-Shaped Fractal Antenna



V. V. Reddy, K. Ashoka Reddy, B. Ramadevi, A. Vijaya, and B. Komuraiah

Abstract A pentagon-shaped patch structure is suggested for dual-band circular polarization (CP) emission. CP is attained by inserting fractals along the sides of the pentagon. Three different structures—without fractals (antenna 1), with Koch fractal (antenna 2), and with Minkowski fractal (antenna 3)—are studied for dual-band CP operation. Antenna with Minkowski fractal of indentation depth 5 mm is experimentally tested and observed to be resonating at 1.8 and 2.7 GHz frequencies with axial ratio (AR) bandwidths of 2.5 and 7.2%. The studied antenna is suitable for GSM and WiMAX applications.

Keywords Dual band · Circular polarization · Fractal · Indentation depth · GSM · WiMAX

1 Introduction

The handheld devices have increasing range of services and related applications attracting the antenna designers to examine the multifunctional antennas. Patch antennas are most suitable for these gadgets because of their pulling features like light weight, low profile, and cheaper cost. Due to the improvements in the current fabrication technology, antenna engineers have proposed a variety of structures in order

V. V. Reddy (✉) · K. Ashoka Reddy · B. Ramadevi · A. Vijaya · B. Komuraiah
Department of ECE, KITSW, Warangal, India
e-mail: vvr.ece@kitsw.ac.in

K. Ashoka Reddy
e-mail: kar.ece@kitsw.ac.in

B. Ramadevi
e-mail: brd.ece@kitsw.ac.in

A. Vijaya
e-mail: av.ece@kitsw.ac.in

B. Komuraiah
e-mail: bk.ece@kitsw.ac.in

to get enhanced bandwidth, gain, and dual band with circular polarization. Circular polarization (CP) is mostly useful in wireless communications like WLAN and Wi-Fi since it can overcome reflection, absorption, and multipath fading problems better than linear polarization.

A stacked dual-band antenna is proposed by Sun et al. [1] to operate at GPS frequencies. Circular polarization is obtained by placing two concentric annular-ring patches on the opposite sides of a substrate. Similar method is examined by Liao [2] with circular-shaped patch on one side and other side a narrow annular ring located, which have small differences in radius for CP. The measured AR bandwidths are 0.65 and 1.04%. Noghabaei et al. [3] have studied crooked slot and truncated corners to generate circular polarization for WiMAX applications. The AR bandwidths are 2 and 3.2% at lower and upper frequency bands correspondingly. A simple square patch antenna with S-shaped slot at the center is investigated by Nasimuddin et al. [4] with aperture coupled feeding mechanism. H-shaped slot on the patch generates multiple bands [5] for GPS, Wi-Fi, and handheld devices applications. Gyun [6] nominated hexagonal-shaped antenna with multiple L-shaped slots to exhibit tri-band behavior. A dual-band CP antenna for handheld RFID reader applications is suggested by Liu et al. [7]. A novel dual-band CP antenna is suggested by Liang et al. [8]. Pin-loaded CP antenna is suggested by Zhang et al. [9]. Along the diagonals, shorting pins are inserted for CP emission.

Fractals are applied to the microstrip patch structures to minimize the size of the antenna and as well as for multiband operation. Multiband operation can be achieved by utilizing fractal curves to the wire antennas. In this paper, a pentagon-shaped antenna is proposed for dual-band operation. Here, fractal curves are employed to the patch structure for multiband radiation. Replacing sides of the antenna with fractal curves generates circular polarization in both the bands. Probe feeding is used to excite the antenna.

2 Antenna Configuration

Fractal geometries are usually specified by two arguments: iteration order (IO) and indentation factor (IF). Koch and Minkowski are two famous fractals used in antennas. The Koch curve geometric construction initiated with a straight line referred to as initiator which is partitioned off into three equal length segments. Then, the middle segment is substituted with two straight lines of same length forming a triangular shape. Minkowski starts with the straight line of length L and is made into 3 equal parts as shown in (Figs. 1 and 2).

Bandwidth of patch antenna is decided by number of current distribution paths on the patch. Initially, a circular patch of diameter 64 mm is simulated. This will generate only one current distribution path. A pentagon with slight variation in sides resonates at more than one frequency. A pentagon of same size is taken as basic patch. Each side of a pentagon can be calculated from $d = 1.17 * r$, where “ r ” is the radius of circle and “ d ” is side of pentagon. The geometry of basic pentagon-shaped patch

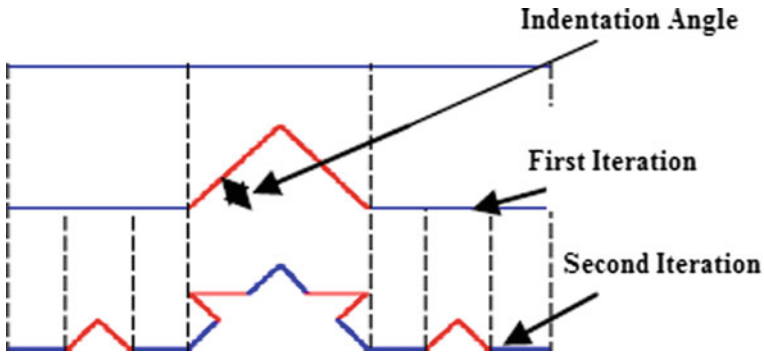


Fig. 1 Generation of Koch curve

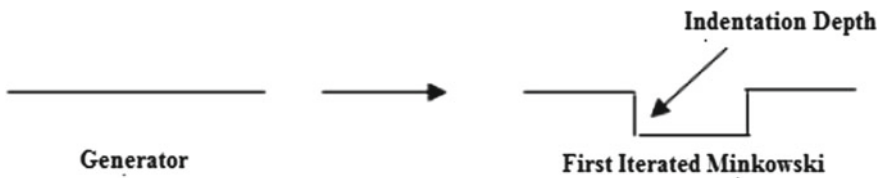


Fig. 2 Generation of Minkowski curve

(antenna 1) is depicted in Fig. 3. The specifications of the antenna considered are as follows: Substrate thickness (h) is 3.2 mm, dielectric constant is 2.2, loss tangent is 0.0019, and each side of pentagon is 39 mm.

Antenna 1 is resonating at two frequencies 1.92 and 3.08 GHz with linear polarization at both the bands. Five sides of the pentagon patch are interchanged with Koch fractal curve to design antenna 2. Indentation factor of Koch curves is indentation angle (IA). Antenna 2 is simulated with three different indentation angles (30° , 45° , 60°). With this structure, CP is achieved only at first frequency band. To design antenna 3, sides of the antenna 1 are replaced with first iterated Minkowski fractal. Antenna 3 generates circular polarization in two bands maintaining good gain.

3 Simulation Results

Antenna 1 resonates at 1.92 and 3.08 GHz with return loss of -39.47 dB and -33.77 dB (Fig. 4). Fractal curves increase electrical length (L) of the patch and also change the direction of currents on the patch. Increase in “ L ” decreases the resonant frequency. Antenna 2 is simulated with different indentation angles, and their return loss characteristics are compared in Fig. 5. Antenna with Koch fractals (antenna 2) resonates at low frequencies compared with antenna 1. From the return loss curve, it

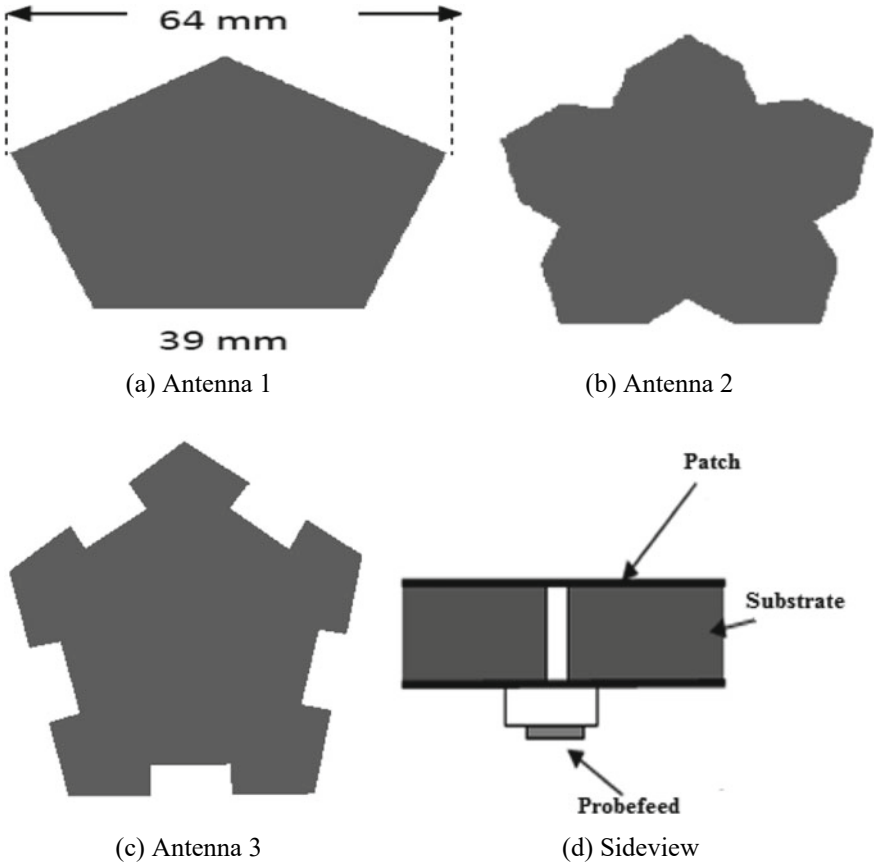


Fig. 3 Side and top views of proposed antenna

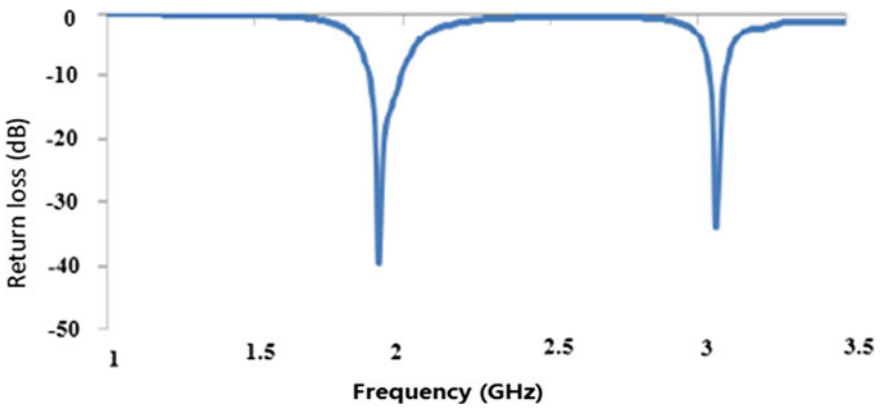


Fig. 4 Return loss for basic pentagon

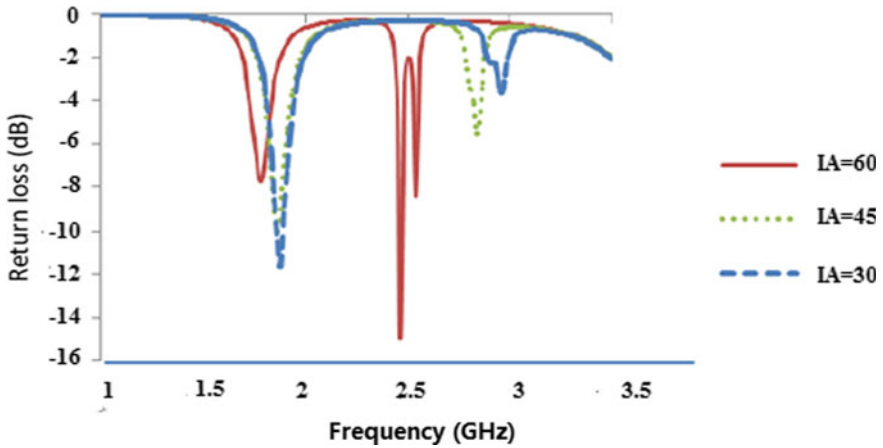


Fig. 5 Return loss curves of antenna 2 for various indentation angles

is observed that for antenna 2 CP is achieved in lower band, whereas in higher band, return loss does not reach the minimum acceptable return loss (-10 dB).

The basic idea behind using Minkowski fractals is to enhance the bandwidth. The indentation factor for Minkowski curve is its indentation depth (ID). Antenna 3 with three different IDs of 2, 5 and 10 mm is simulated and compared in Fig. 6. From the figure, it is observed that antenna 3 with ID = 2 and 5 mm generates CP in both the bands. The performance of the antenna degraded for ID = 10 mm. Axial ratio bandwidths for ID = 2 mm are 2.2 and 1.7%, whereas for ID = 5 mm, it is 2.6 and 7.8%. The bandwidth of 3-dB axial ratio is increased in second band due to increase in ID.

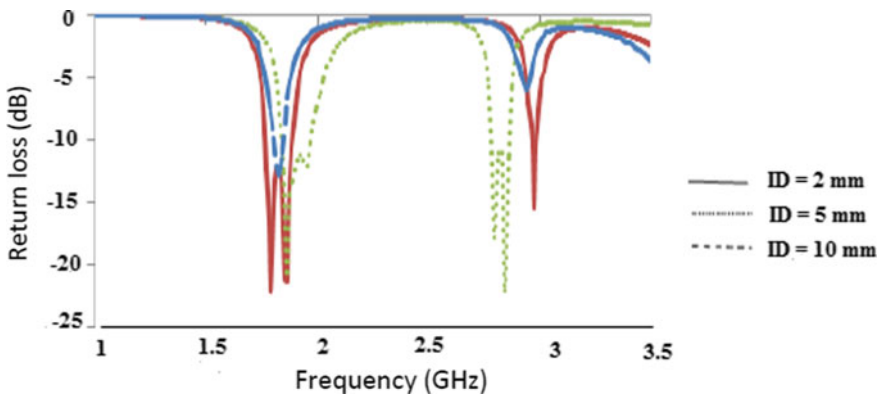


Fig. 6 Return loss characteristics of antenna 3 for various indentation depths

4 Measured Results

The best performed proposed antenna 3 with ID = 5 mm is fabricated, and experimentations are carried in defense laboratory. The proposed geometry is etched on a RT/duroid 5880 material of thickness 3.2 mm. Prototype of fabricated antenna is depicted in Fig. 7. The comparison of measured and simulated return loss results is given in Fig. 8. The axial ratio results are shown in Fig. 9. The 3-dB axial ratio bandwidth is obtained in the frequency bands of 1778–1822 MHz and 2603–2797 MHz.

Fig. 7 The photograph of the fabricated antenna 3 with ID = 5 mm

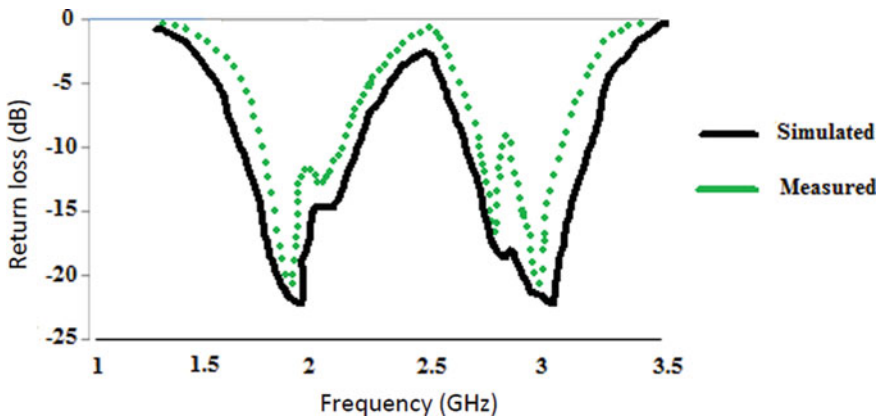
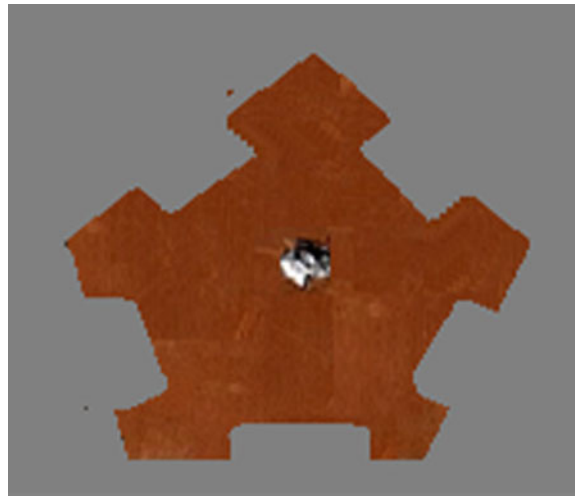


Fig. 8 The comparison of return loss curves of the fabricated antenna 3

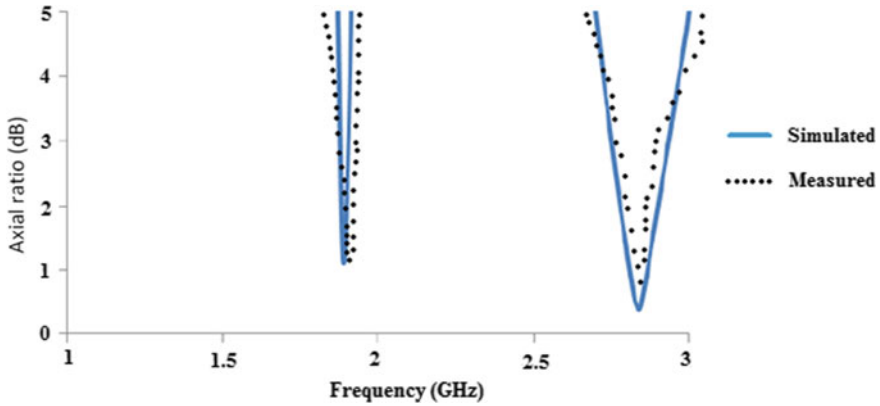


Fig. 9 The comparison of axial ratio plot for antenna 3 with ID 5 mm

5 Conclusion

A dual-band CP antenna is nominated using pentagon shape as basic patch. Koch and Minkowski fractals are applied to this patch with different indentation factors. Simulated results show that when sides of normal patch are replaced with Minkowski fractals, desirable circular polarization is generated. The axial ratio bandwidth for ID = 5 mm is 45 MHz for lower band and 164 MHz for upper band, and maximum gain is 6.8 dB. The proposed antenna suits well for GSM and WiMAX applications.

References

1. Zhang XSZ, Feng Z (2011) Dual-band circularly polarized stacked annular-ring patch antenna for GPS application. *IEEE Antennas Wirel Propag Lett* 10:49–51
2. Liao W, Chu QX (2010) Dual-band circularly polarized microstrip antenna with small frequency ratio. *Progress Electromagnetic Res Lett* 15:141–152
3. Noghabaei SM, Abdul Rahim SK, Soh PJ, Abedian M, Vandenbosch GA (2013) A dual-band circularly-polarized patch antenna with a novel asymmetric slot for WiMAX application. *Radio-engineering* 22(1):291–295
4. Chen ZN, Qing X (2010) Dual-band circularly polarized S-shaped slotted patch antenna with a small frequency-ratio. *IEEE Trans Antennas Propag* 58(6):2112–2115
5. Chang TH, Kiang JF (2013) Compact multi-band H-shaped slot antenna. *IEEE Trans Antennas Propag* 61(8):4345–4349
6. Baek JG, Hwang KC (2013) Triple-band unidirectional circularly polarized hexagonal slot antenna with multiple L-shaped slits. *IEEE Trans Antennas Propag* 61(9):4831–4835
7. Liu Q, Shen J, Yin J, Liu H, Liu Y (2015) Compact 0.92/2.45-GHz dual-band directional circularly polarized microstrip antenna for handheld RFID reader applications. *IEEE Trans Antennas Propag* 63(9):3849–3856

8. Liang ZX, Yang DC, Wei XC, Li EP (2016) Dual-band dual circularly polarized microstrip antenna with two eccentric rings and an arc-shaped conducting strip. *IEEE Antennas Wirel Propag Lett* 15:834–837
9. Zhang X, Zhu L, Liu NW (2016) Pin-loaded circularly-polarized patch antennas with wide 3-dB axial ratio beamwidth. *IEEE Trans Antennas Propag* 65(2):521–528

Device Design and Modeling of Fin Field Effect Transistor for Low Power Applications



Umamaheshwar Soma, E. Suresh, B. Balaji, and B. Ramadevi

Abstract Fin field effect transistor (FinFET) is the newest technology compared to metal oxide semiconductor field effect transistors (FET), and we designed various structures of FinFETs as double-gate FETs, trigate FETs, and gate all around field effect transistor in nanometer technology using Silvaco TCAD tool. In this work, we developed a novel structure of FinFETs for various low power VLSI applications with all DC and AC improved parameters such as on current, off current, threshold voltage, drain conductance, transconductance, and on resistance.

Keywords Metal oxide semiconductor · FinFET · Nanometer · VLSI applications · Transconductance

1 Introduction

As the technology develops year to year as per the Moore law, it all goes to the benefits of the FinFET technology. As we want to switch to the newest technology as FinFET, initially, we will see the main drawbacks of conventional complementary metal oxide semiconductor (CMOS) [1]. So we need to move toward the FinFET. Before starts, the structure of a CMOS consists of a p-type of substrate two sources and a drain terminal [2]. To apply drain voltage due to applications of drain voltage, there will

U. Soma (✉) · E. Suresh · B. Ramadevi
Department of ECE, Kakatiya Institute of Technology and Science, Warangal 506015, India
e-mail: sum.ece@kitsw.ac.in

E. Suresh
e-mail: esuresh77@gmail.com

B. Ramadevi
e-mail: ramadevikitsw@gmail.com

B. Balaji
Department of ECE, Koneru Lakshmaiah Education Foundation, Green fields, Vaddeswaram,
Guntur Dist. 522502, India
e-mail: balaji@kluniversity.in

be an induced current from source to drain terminal [3–5]. Here, we will talk about induced current from the source to drain whereas carriers from the substrate to the source and drain [6], then there will be no conduction of current due to applied gate voltage but not due to the drain voltage [4] so the barrier is shifting, i.e., lowering due to gate voltage. In case of long channel MOSFET, the applied gate voltage forms the channel. If the drain voltage is applied across the barrier, it lowers due to the gate voltage which is undesirable characteristics of MOSFET, whereas for the short channel if we apply the little bit of drain voltage which is equal to long channel MOSFET, whereas if we increase the increased drain voltage barrier is lowering which induces barrier induced drain voltage (BIDL) [7].

2 General Structure

If we increase the drain current, then there is an n -times increase in drain current in both OFF and ON states. And the sub-threshold slope remains the same [8].

Long channel MOSFET characteristics:

- Threshold voltage remains the same.
- Sub-threshold slope remains same.
- ON and OFF current increases with drain voltage in the same proportion.
- Short channel MOSFET characteristics:
- Drain induced barrier lowering (DIBL) due to V_T .
- Sub-threshold voltage changes.
- Off current increases (leakage current increases).

In short channel MOSFET, the I_d drain voltage is increased by 100 times, then ON current increases by 100 times but OFF current increases more than 100 times because of a decrease in the barrier. And threshold voltage also shifts with the applications of drain voltage.

Figure 2 shows that if we increase the drain current, then there is an n -times increase in drain current in both OFF and ON states [9]. And the sub-threshold slope remains the same for novel devices [10]. The cross-sectional view along the channel direction is shown in Fig. 1. Here, the heavy dopant source and drain regions are calculated to be epitaxial regrowth, therefore, the source to drain regions of the FinFET do not comprise inserted-oxide layers.

The FinFET can be fabricated using different processing steps such as initially the substrate on which it is fabricated should be deposited on hard mask. Once the hard mask is deposited, then the process of etching completes the process. Gate deposition is the most important process throughout it [11] (Fig. 3).

The performance characteristics of a FinFET are considerably promising at the end of MOSFET and also gate all around field effect transistor for metal oxide semiconductor field effect transistor in both channels. The drain current is increased with increase in drain voltage [12] and calculated various its performance parameters for both analysis [13] (Fig. 4).

Fig. 1 General structure of conventional MOSFET

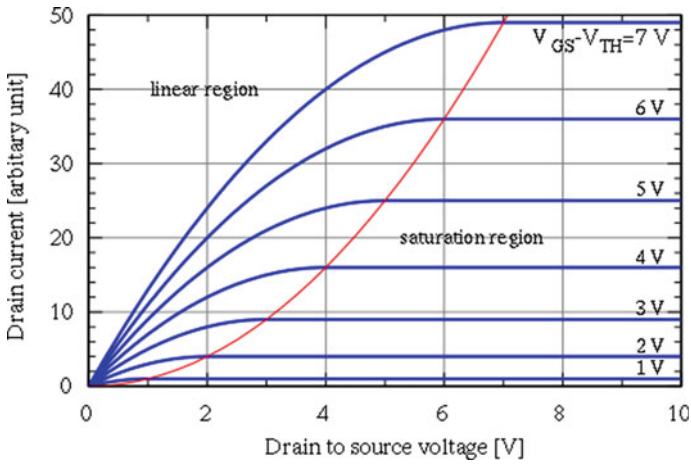
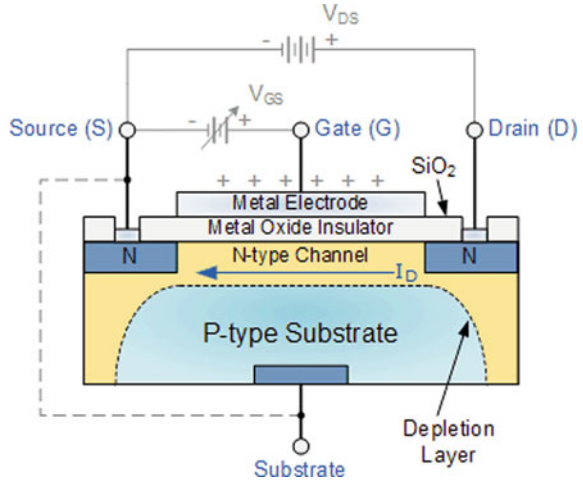


Fig. 2 I_d versus V_{GS} characteristics of long channel MOSFET

Fig. 3 I_d versus V_{GS} characteristics of short channel MOSFET

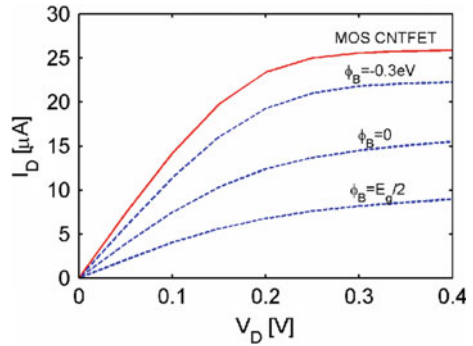
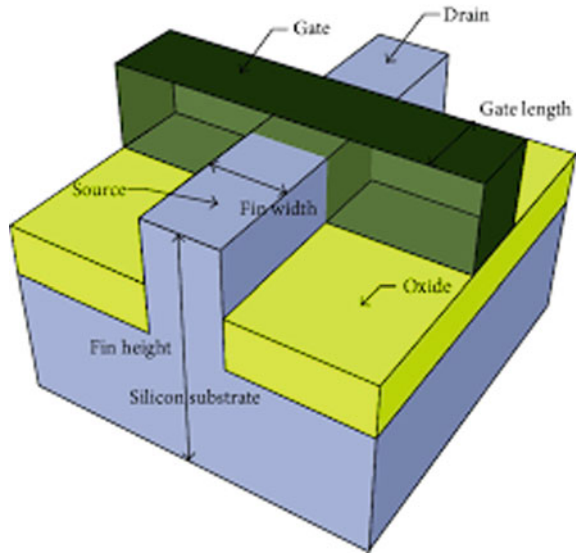


Fig. 4 MOSFET scaling parameters



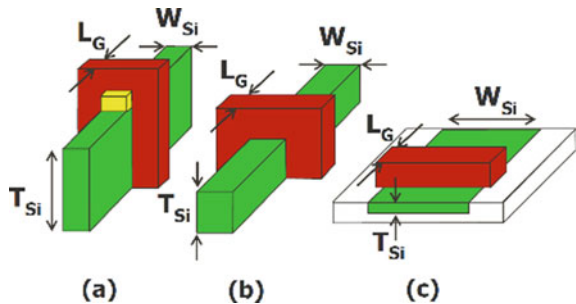
MOSFET scaling issues:

- Leakage current is serious issue for scaling.
- To suppress leakage, there is a need to deposit higher body doping and lower carrier mobility, higher capacitance.

Here, Fig. 5 shows the three-dimensional figure of FinFET, basically similar to the planar MOSFET except that the fin is completely wrapped on to the channel in three directions from source to drain. The structure is a non-planar structure [14], i.e., a non-planar double-gate transistor built on SOI. Characteristics of FinFET is the complete conducting channel wrapped by a thin Si fin which forms the body of the device.

The thickness of the fin is determined by the effective channel length of the device. If more gates are added, i.e., one above and one below (DG-MOSFET), or also put at the side (TG-FINFET) or if we put gate all around (GAA FinFET), then control

Fig. 5 MOSFET scaling parameters



over current flow can be increased. FinFET devices have two gates only. From the top gate, there is no effect on the channel, but from the sides only whereas trigate, currently controlled from the three sides of the channel.

3 Result Analysis

In planar MOSFET, gate controls the current from only one direction and the structure is the same as the triple gate FinFET. In a triple gate, the gate is completely controls the current from the three sides of the fin, where the fin is a common channel in between. In double-gate FinFET, the hard mask is connected on top of the fin so electric fields which are coming from the gate are completely controlled by both sides of the gates but not from the top gate [15]. Whereas in triple gate FinFET, the electric field coming from the gate is completely controlled by the three sides of the gates where the box is buried oxide layer [16] (Fig. 6).

In shorted gate, the gate is shorted on above and below on the substrate and basically, [11] we will call it a three-terminal FinFET whereas in an independent gate both gates are independent to each other and having four terminals and occupy more area than shorted gate FinFET.

In SOI FinFET, the fin is starting from the oxide surface and gate oxide material. It means that bulk and fin directly not connected [17]. In bulk FinFET, fin is starting from the wafer, then it is moving, and besides that, there is SiO₂, after that gate oxide material is deposited (Figs. 8, 9 and 10) (Table 1).

Fig. 6 Double-gate FinFET

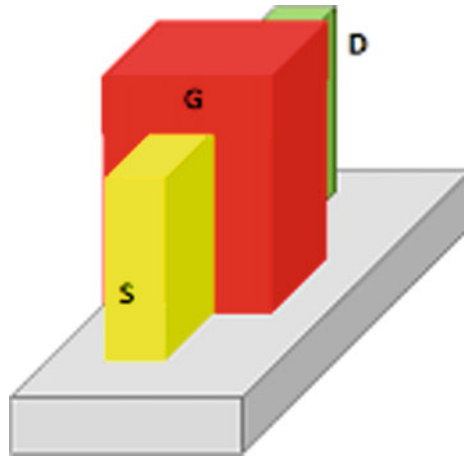


Fig. 7 DIBL with oxide thickness characteristics

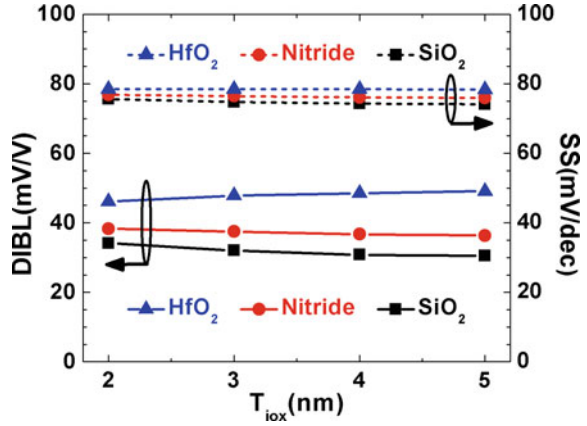


Fig. 8 Threshold voltage at various channel length

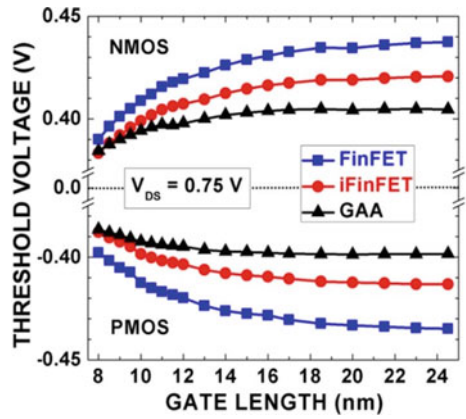


Fig. 9 Simulated transconductance characteristics

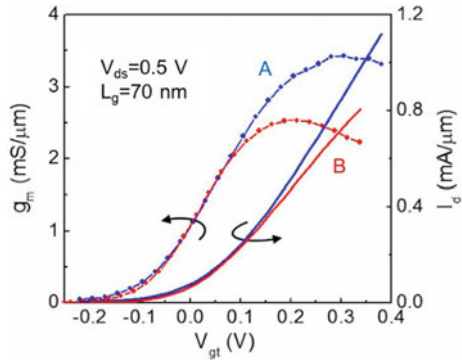


Table 1 Parameters used in the device

Device parameter	FinFET
Gate length (nm)	12
Fin width (nm)	6
Total Si height (nm)	18
Gate pitch (nm)	35
Equivalent oxide thickness (nm)	0.7
Oxide thickness (nm)	3
Metal thickness (nm)	6
Resistivity ($\Omega\text{-cm}^2$)	3.5×10^{-9}

4 Conclusion

In this paper, the novel structures of fin field effect transistor for the double-gate transistor, triple gate transistor, and gate all around transistors in deep submicron technology are developed and have calculated various improved parameters as on current, off current, threshold voltage, drain conductance, transconductance, and on resistance.

Acknowledgements The authors would like to thank National Institute of Technology Silchar for providing necessary computational tools.

References

1. Aditya M, Rao IV, Balaji B, John Philip B, Ajay Nagendra N, Krishna SV (2019) A novel low-power 5th order analog to digital converter for biomedical applications. *Int J Innov Technol Exploring Eng* 8(7):217–220
2. Balaji B, Aditya M, Adithya G, Sai Priyanka M, Ayyappa Vijay VVSSK, Chandu K (2019) Implementation of low-power 1-bit hybrid full adder with reduced area. *Int J Innov Technol Exploring Eng* 61–64
3. Kumar PK, Balaji B, Rao KS (2022) Performance analysis of sub 10 nm regime source halo symmetric and asymmetric nanowire MOSFET with underlap engineering. *Silicon*. <https://doi.org/10.1007/s12633-022-01747-y>
4. Aditya M, Veeraraghava Rao I, Balaji B, John Philip B, Ajay Nagendra N, Vamsee Krishna S (2019) A Novel Low-Power 5th order Analog to Digital Converter for Biomedical Applications. *Int J Innov Technol Exploring Eng* 217–220
5. Sravani SS, Balaji B, Rao KS et al (2022) A Qualitative review on tunnel field effect transistor-operation, advances, and applications. *Silicon*. <https://doi.org/10.1007/s12633-022-01660-4>
6. Naraiah R, Balaji B, Radhama E, Udutha R (2019) Delay approximation model for prime speed interconnects in current mode. *IJITEE* 8(9):3090–3093, ISSN: 2278-3075
7. Sravani KG, Prathyusha D, Rao KS, Kumar PA, Lakshmi GS, Chand CG, Naveena P, Thalluri LN, Guha K (2019) Design and performance analysis of low pull-in voltage of dimple type capacitive RF MEMS shunt switch for Ka-band. *IEEE Access* 7:44471–44488
8. Aditya M, Rao KS, Balaji B et al (2022) Comparison of drain current characteristics of advanced MOSFET structures—a review. *Silicon*. <https://doi.org/10.1007/s12633-021-01638-8>

9. Girija Sravani K, Koushik Guha, Srinivasa Rao K (2020) A modified proposed capacitance model for step structure capacitive RF MEMS switch by incorporating fringing field effects. *Int J Electron* 1–22
10. Girija SK, Srinivasa Rao K (2018) Analysis of RF MEMS shunt capacitive switch with uniform and non-uniform meanders. *Microsyst Technol* 24(2):1309–1315
11. Balaji B, Rao KS, Sravani KG et al (2022) Design, performance analysis of GaAs/6H-SiC/AlGaIn metal semiconductor FET in submicron technology. *Silicon*. <https://doi.org/10.1007/s12633-021-01545-y>
12. Balaji B, Ajaynagendra N, Radhamma E, Murthy AK, Kumar MK (2019) Design of Efficient 16 Bit Crc with optimized power and area in Vlsi circuits. *Int J Innov Technol Exploring Eng* 87–90
13. Balaji B, Rao KS, Aditya M et al (2022) Device design, simulation and qualitative analysis of GaAsP/6H-SiC/GaN metal semiconductor field effect transistor. *Silicon*. <https://doi.org/10.1007/s12633-022-01665-z>
14. Alluri S, Balaji B, Cury C (2021) Low power, high speed VLSI circuits in 16nm technology. *ISSN: 0094-243X*, vol 2358, issue 1, July 2021, pp 030001-1–16. <https://doi.org/10.1063/5.0060101>
15. Rao KS, Naveena P, Sravani KG (2019) Materials impact on the performance analysis and optimization of RF MEMS switch for 5G reconfigurable antenna. *Trans Electr Electron Mater* 20(4):315–327
16. Balaji B, Ajay Nagendra N, Radhamma E, Krishna Murthy A, Lakshmana Kumar M (2019) Design of efficient 16 bit Crc with optimized power and area in Vlsi circuits. *IJITEE* 8(8 June 2019):87–91, *ISSN: 2278-3075*
17. Alluri S, Mounika K, Balaji B, Mamatha D (2021) A novel implementation of 4 bit parity generator in 7nm technology. *ISSN: 0094-243X*, vol 2358, issue 1, July 2021, pp 030002-1–10. <https://doi.org/10.1063/5.0059329>

A Secure Biometric Novel Approach for Authentication Using Multi-Fingerprint Traits



Manoj Kumar Vaddepalli and Adepu Rajesh

Abstract With the rapid enhancements in the technology era, high-end security systems are necessary to authenticate the correct user. Biometric-based automatic authentication facilities are in demand to solve the security issues. Among all biometrics, fingerprint authentication is the most and widely accepted approach. Though several applications with a fingerprint are supporting the authentication but yet are not attaining confidence even though combined with some personal identification number. The single fingerprint image used for authentication can be obtained with modern techniques to break the security. In this paper, a novel method is presented by considering the fusion of five fingerprint images. Each fingerprint image is preprocessed individually and to improve the security performance, all the five fingerprint minutiae points are hashed and it is applied to decide the user authentication. The hashed-based vector is stored in the database. The approach preprocessing the images separately involves feature extraction. The last fingerprint image is only obtained for the security break but with our approach, it is not possible to break the security as it needs five fingerprints. The method certainly improves the level of security.

Keywords Finger print image · Authentication · SHA-3 · Security

1 Introduction

Biometric system identification is an automatic recognition which prohibits unauthorized user. The biometric system possesses a sensor to capture fingerprint images, minutiae feature extraction, matching, and decision [1].

M. K. Vaddepalli (✉)

School of Computer Science and Artificial Intelligence, SR University, Warangal, TS, India
e-mail: manoj02526@gmail.com

A. Rajesh

Department of Computer Science and Engineering, Guru Nanak Institute of Technology, Hyderabad, TS, India

1.1 Biometric System Identification

In the domain of information technology, easy and widely available information must be secure [2–5]. Integrity and confidentiality are critically important. Accurate automatic personal identification is necessary for various applications like driving license, passports, ATM, cellular telephones, etc. The earlier methods for identification and validation that happen using PIN /Password were unreliable, reliable solution to these problems was rectified by using biometric features. Universality, acceptability, distinctiveness, performance, permanence, measurability are some of the biometric characteristics [4–6].

1.2 Biometric System Applications

Biometric systems are found in numerous applications [5]. Some of them are:

Government applications—national ID cards, driving license, passports, and welfare schemes.

Commercial applications—e-commerce, ATM or Credit cards, forensic applications—criminal investigation, parenthood determination, and terrorist identification.

1.3 Finger Print Features

Fingerprints are mostly used in biometric systems and are unique. Ridges are the lines in the fingerprint, and the space between ridges is a valley. The most prominent local characteristics of the fingerprint includes ridge ends and bifurcation where a ridge forks or diverges into branch ridges. Figure 1 depicts the ridge ending, bifurcation, and other features of the fingerprint.

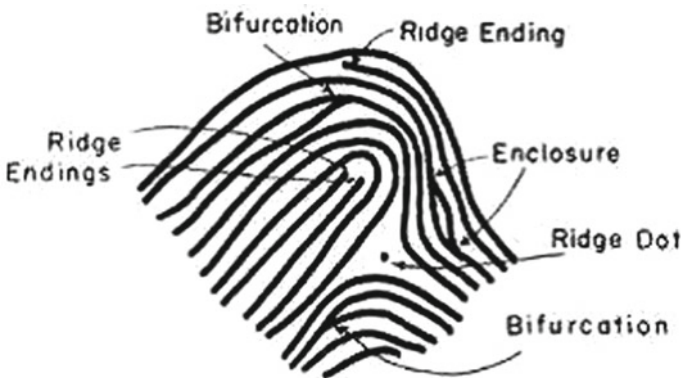


Fig. 1 Finger print features

2 Literature Review

Proposed a new offline products purchase approach that eliminates the use of smart-phone transaction services and wallets. The approach uses a hash-based minutia encryption technique with a four-digit secure pin. Elgamal cryptosystem and SHA-512 algorithms are used for encryption and decryption of minutiae points. In this approach, the session key is used for encrypting the concatenated minutiae points, pin, and the resultant is again encrypted by server's public-key. This encrypted data is transferred to the server, next, the server decrypts the received encipher data by its private-key followed by session key which is shared at the time of communication and obtains original minutiae points and pin. Minutiae point approach reduced the attacks up to a great extent [1, 7].

Demonstrated how the support vector machine designs a fingerprint recognition system for capturing the minutiae characteristics of a fingerprint image. The imaging system converts each fingerprint image into finger code by Gabor filters. Instead of more conventional image processing and pattern recognition techniques, the processing architectures developed by SVM perform better in many cases [8]. This level of performance possible by elucidating the computational principles [9].

Discussed the fingerprint minutiae points matching based on local and global structures, the procedure uses minutiae's local and global structure. The local structure describes the translation and rotation invariant feature of the minutia in its neighborhood. Reliability of global matching is increased by finding the correspondence of two minutiae sets and global minutiae structure to determine the uniqueness of the fingerprint. The fusion of local and global structures makes a minutiae matching more reliable and robust. Due to its high processing speed, it is suitable for online processing [2, 10–12].

Proposed a circular technique to identify the minutiae points. The picture border is calculated after thinning the four extreme points. A rectangle is generated using these four extreme points and a middle point was also extracted. The lowest distance between the middle point and the extreme four points is calculated and used as the radius for drawing the circle. Based on the calculated middle point, the circle was drawn which stores the distance of the points for the recognition of the user. The authors not considered the growth of fingers and this circular technique is not advisable for partial fingerprint recognition too [3].

Presented fingerprint recognition based on feature fusion and pattern entropy. For each minutiae location, multiple orientation values were assigned to protect from rotation and scaling. And Gaussian weight-based feature point matching was used to eliminate the spurious minutiae caused by noise in incomplete regions [13]. False matching rate (FMR) was alone calculated, which performed better compare to minutiae matching and orientation field-based matching algorithm. For the protection of rotation and scaling multiple orientation, values were assigned for minutiae location, and it needs more space for storing minutiae information [4].

Enlighten the contemporary status of tolerability, evidence acquirement, and jurisdiction in social media forensics and depicted the instantaneous challenges in the

collection and analysis. They suggested machine learning procedures are helpful toward information grouping, association, and investigation. A hash analysis is presented in image matching [14].

Concise digital forensics concepts, the different segments of digital forensics, and also the comparison are illustrated on these tools. They briefed about the danger of cybercrime is in the networks. Beginning with phishing to lacerating and so on. Furthermore, the paper foretells and presents patterns of emergency in computerized criminological those have been recognized by numerous eyewitnesses [15, 16].

3 Methodology

3.1 Proposed Design

Fingerprint authentication is much broader and wider in applications of scientific and engineering [3]. The minutiae image of the fingerprint is converted into a vector code using the techniques to identify a person. There is a chance of tampering single biometric fingerprint minutia features in identification. To avoid this, multi-fingerprint images are necessary to authenticate the individual. We propose a novel high secure method that uses five fingerprint image features. Here only the last fingerprint image can tamper with modern technologies which are not sufficient to break the security of authentication. The order of fingerprint image scanning is completely based on the user's interest to achieve higher security. During authentication of the user, the same order is to be followed.

3.2 Procedure

Minutiae points extraction: The fingerprint image features like ridge ending, ridge bifurcation, etc., are generally used in finding the minutia points. These are present in the form of points having x and y coordinates. The following algorithm is applied to find the minutia points.

Algorithm: Minutia Points

Input: { Fingerprint Image: FP }

Output: {Minutia Points: MP }

Read(FP)

FB \leftarrow Binarization (FP)

FT \leftarrow Thinning (FB)

Minutia points \leftarrow FT

FT# \leftarrow Removal of false minutia points (FT)

MP \leftarrow Orientation(Region Selection(FT#))

Binarisation: is the process that obtains a binary image from a gray level image where black pixels represent ridges and white pixels as valleys. Morphological operations may be used to remove unnecessary spurs line breaks and bridges.

if GrayLevel(Pixel value) $> \lambda$ then

pixel value = 1

else

pixel value = 0

Thinning is used to remove duplicate pixels of ridges by marking in a small window. Thus each ridge will be one pixel wide. Then the minutiae points are marked using the cross-number concept. That is, scanning each ridge pixel neighborhood. Consider a 3×3 window. The ridge end is marked if the central pixel is 1 and it has only one neighbor. Ridge bifurcation is marked if the central pixel is one and it has 3 one value neighbors [17]. False minutiae points are eliminated by applying the Euclidean distance method. Region selection is performed by morphological operations: Open and Close. This is a subset of an image. Based on the image dimensions, centroid value is calculated. From this region, selection is obtained to calculate the Orientation() [18].

3.2.1 Registration

Biometric device captures all the five fingerprint images of the user and stores them at buffer. The preprocessing techniques—binarization, thinning, and noise removal techniques applied to each image read.

The preprocessed minutiae's of each image concatenated as follows: First fingerprint minutiae points are hashed using SHA-3, the resultant hash value attached to second fingerprint minutiae points, that total will again get hashed using SHA-3 [19]. This process will repeat to all other fingers and generate one single hash value. This hash value can be considered as an identifier for the customer in the database [20].

Training Steps:

Input: Fingerprint images

Output: Registration

// HashValue is either 0's or 1's initially.

Begin

Repeat for all five fingerprint sets do

For fingerprint image 1 to 5 do

Preprocess the images

Extract minutiae features

End For

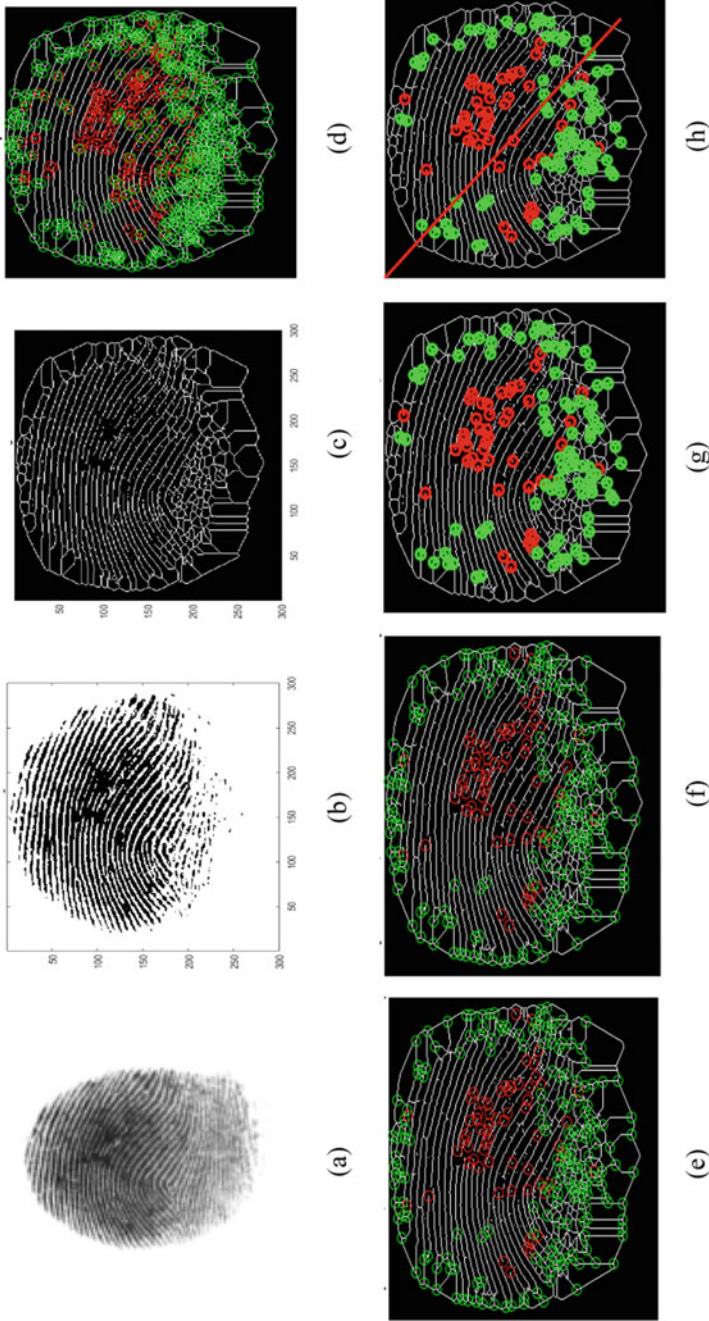


Fig. 2 A Finger print image. **b** Binarized image. **c** Fingerprint image after thinning. **d** Identification of minutiae points. **e** Minutiae points after removing false minutiae. **f** Selection of ROI. **g** Minutiae points orientation. **h** Threshold line for assigning binary values to Minutiae points

```

For MinutiaePoints of image 1 to 5 do
HashValue = HashValue + (MinutiaePoints of image[i])
HashValue = SHA3(HashValue)
End Repeat
End
    
```

Testing Steps:

```

Input: Fingerprint images
Output: User authenticated or denied
Begin
    for fingerprint image 1 to 5 do
        Preprocess the images
        Extract minutiae features
    end for
    for MinutiaePoints of image 1 to 5 do
        HashValue = HashValue + (MinutiaePoints of image[i])
        HashValue = SHA3(HashValue)
    Check in the data store
    Obtain Decision
    if Decision =FOUND
        User Authenticated
    else
        User denied
    End
    
```

3.2.2 Authentication

To validate the proposed method, Algorithm Authentication is used.

Algorithm Authentication :

```

Initialization: {Fingerprint FP; Database: DB,User :U, Authentication: AU}
Input : {FP}
Output: {AU}
    for FP->FP1 to FP5 do
    Begin
        Preprocess(FP)
    end for
    Concatenate and Hash(FP)
    Set HashValue->DB
    if HashValue εDB then
    Allow<=AU(U)
    else
        Not Allow <=AU(U)
    endif
    
```

4 Security Analysis

The results of the proposed work presented in the form of security analysis. The approach presented in this paper shows the authentication level of the customer. The procedure uses the first fingerprint minutiae points of the customer. These points are hashed and concatenated with another fingerprint minutiae points. After that resultant value gets hashed, this will repeat until all fingerprints are covered. The final hash value can use to identifies the customer uniquely, which is stored in the database. This approach uses hashing, which will provide high security:

By using a single fingerprint, there is the possibility of capturing that finger from the device. But the proposed approach capturing several fingerprints one by one. By this, attacker will get only one fingerprint by which he cannot authenticate.

X1, X2, X3, X4, and X5 are fingerprint image minutiae points in one order and are stored in the database as follows:

$$DB \leftarrow (H(H(H(H(H(X1). X2). X3). X4). X5).$$

In this approach, the order of fingerprints also provides more security even the attacker gets all fingerprints without knowing the proper order of fingerprints. By that, the attacker cannot authenticate him/herself.

If the attacker attacks the server, he won't get the credentials of the customer, because the user credentials are hashed, which is not possible to get the credentials from that.

5 Conclusion

Privacy is the most concern in the area of authentication, and biometric features are playing a prominent role. Fingerprint authentication is the most used and reliable. The paper proposed a novel approach with multi-finger biometric incorporating the hash function to individual fingerprint minutiae points. The algorithms presented in this paper are more effective and found to be feasible with reliability. In the approach, we used five fingerprint minutiae points. Based on the application and requirements in the application, the approach can use either three, four, or more than five also. The strength of the privacy can be enhanced by using more than five fingerprints.

References

1. Vaddepalli MK, Rajesh A, Yamsani N (2020) Secure off-line shopping using fingerprint biometric approach. *Int J Adv Sci Technol* 29(5):8667–8673
2. Jiang X, Yau WY (2010) Fingerprint minutiae matching based on the local and global structures. In: *International conference on pattern recognition*, vol 2. Jan 2010
3. Bhattacharya S, Chakraborti S, Mali K (2013) Revolutionary extended spatial point extraction using circular technique (RESPECT). *Int J Comput Sci Eng (IJCSSE)* 5(7):672–677

4. Jie Z, Xiao J, Na C, Jian-li W (2013) Incomplete fingerprint recognition based on feature fusion and pattern entropy. *J China Univ Posts Telecommun* 20(3):121–128
5. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. *IEEE Trans Circuits Syst Video Technol Special Issue on Image- and Video-Based Biometrics* 14(1) (January)
6. Golfarelli M, Maio D, Maltoni D (1997) On the error-reject trade-off in biometric verification systems. *IEEE Trans Pattern Anal Mach Intell* 19(7):786–796
7. Kothandaraman D, Balasundaram A, Dhanalakshmi R, Sivaraman AK, Ashokkumar S et al (2022) Energy and bandwidth based link stability routing algorithm for IoT. *CMC-Comput Mater Continua* 70(2):3875–3890
8. Mansfield AJ, Wayman JL (2002) Best practices in testing and reporting performance of biometric devices. Version 2.01. From communications electronics security group (CESG), Aug 2002
9. Elmira Y, Elberichi Z, Adjoudj R (2012) Support vector machine based fingerprint identification. In: Conference Paper, Nov 2012. <https://www.researchgate.net/publication/233808988>
10. Zang J, Yuan J, Shi F, Du SD (2008) A fingerprint matching algorithm of minutia based on local characteristic. In: Fourth international conference on natural computation, Jan 2008. <https://www.researchgate.net/publication/232640017>
11. Zang J, Yuan J, Shi F, Du SD (2008) A fingerprint matching algorithm of minutia based on local characteristic. In: Fourth international conference on natural computation. IEEE
12. Komuravelly SK, Kanegonda RC, Jamalpur B, Dandugudum M, Yadav BP (2020) A research on security problems with data storage in cloud computing. In: *IOP Conference Series: Materials Science and Engineering*, vol 981.
13. Akuthota I, Sunil G, Sallauddin M (2017) A new method of secure payment solutions fully off-line functions on Frodo. *Int J Eng Technol Comput Res (IJETCR)* 5(4):145–149
14. Reddy ST, Mothe R, Sunil G, Harshavardhan A, Korra SN (2019) Collecting the evidences and forensic analysis on social networks: disputes and trends in research. *J Study Res XI(XII)*:183–192
15. Sandeep CH, Thirupathi V, Pramod Kumar P, Naresh Kumar S (2019) Goals and model of network security. *Int J Adv Sci Technol* 28(20):593–599
16. Akarapu M, Marthi S, Donthamala KR, Prashanth B, Sunil G, Mahender K (2020) Checking for identity-based remote data integrity cloud storage with perfect data privacy. In: *IOP Conference Series: Materials Science and Engineering, ICRAEM 2020*
17. Akram MU, Tariq A, Khan SA, Nasir S (2008) Fingerprint image: pre and post processing. *Int J Biometrics* 1(1)
18. Seshadri R, Trivedi TR (2010) Generate a key for MAC algorithm using biometric fingerprint. *Int J Ad hoc Sens Ubiquit Comput (IJASUC)* 1(4)
19. Gilbert H, Handschuh H (2004) Security analysis of SHA-256 and sisters. In: *Proceedings, CRYPTO '03*. Springer-verlag, Berlin, pp175–193
20. Uludag U, Jain AK (2004) Attacks on biometric systems: a case study in fingerprints. In: *Proceedings of (SPIE), security, steganography, and watermarking of multimedia contents VI*, vol 5306. pp 622–633

Static Hand Gesture Recognition for ASL Using MATLAB Platform



R. Ravi Kumar, Sallauddin Mohmmad, Shabana, D. Kothandaraman, and Dadi Ramesh

Abstract Generally, communication with people in our daily life is by speaking with voice but some communications can be possible with body language, facial expressions, and hand signs. We can also communicate with others without voice. Apart from that, hand gestures are playing very important role in communication. Here, we developed a gesture identification system which interprets the American Sign Language. This system helps the people who are deaf and dumb. This system leads them to understand and communicate as like normal people. Lot of proposals are introduced on gestures specified with their languages like ASL, ISL, etc. Here, we are introducing new static gestures using MATLAB on bases of existing systems. Our input is captured from camera; then, system applies the pre-processing on captured image. The set of features are retrieved using PCA. Comparison of the features is done using Euclidean distance with the help of training sets. Finally, optimal gestures identify and produce the output inwards of text or voice.

Keywords Static gesture recognition · PCA · Euclidean distance · MATLAB software

1 Introduction

Gesture recognition system has been adjusted for different research applications from facial motions to finish substantial human activity. Different applications have developed and made a more grounded requirement for this kind of gesture recognition system [1]. More researches are going on this platform to make human activity easy. This kinds of research also introduced in machine learning, cognitive sciences, and

R. Ravi Kumar (✉) · S. Mohmmad · D. Kothandaraman · D. Ramesh
School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India
e-mail: ravikumar.racha@gmail.com

Shabana
Department of Computer Science and Engineering, Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India

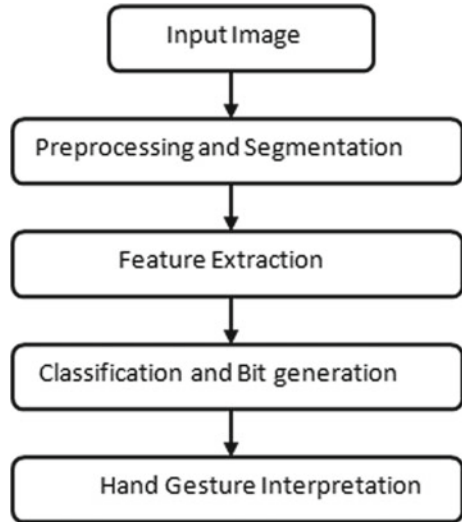
more other advanced technologies. Several proposed strategies for perceiving static and dynamic hand gestures by breaking down the raw streams produced by the sensors connected to human hands. This technique accomplished an acknowledgment pace of more than 75% on the ASL signs [1, 2]. Presently, these kinds of hand gesture systems are using in the smart mobiles. In any case, the client needs to utilize a glove-based interface to extricate the advances of the hand motions which constrains their ease of use in certifiable applications, as the client needs to utilize extraordinary gloves so as to communicate with the framework.

Another examination introduced a real-time static isolated gesture application utilizing a hidden Markov model methodology. The features of this application were separated from signal outlines. Nine diverse hand signals with different degrees of turn were thought off. The drawback of this element extraction strategy is the utilization of skin-based segmentation technique which does not work appropriately within the sight of skin-shaded items out of sight. Gesture-based communication is not just utilized by those in need of a hearing aid and the discourse weakened people to discuss either with one another or the ordinary people; however, it is utilized by numerous individuals to convey [3, 4]. Communication through signing does not mean the utilization of hand signals no one but, it very well may be any sort of sign utilizing any piece of body; it might be eyes, legs, and so on. This language fluctuates from nation to nation. Here, the signs of ASL is utilized for advancement of the framework for acknowledgment of signs [5]. A segment of the issue done by talk and hard of hearing people while talking with regular people were social participation, correspondence dissimilarity, guidance, direct issues, mental wellbeing, and security concerns.

The manners by which one can interface with PC are either by utilizing gadgets like console and mouse or by means of sound signs, while the previous in every case needs a physical contact and the last is inclined to commotion and aggravations. The activity of the body can represent an information with hands, eyes, legs, etc. that will become gesture. Apart from that, hand represented signals are more accurate way to convey the information. In this model, we proposed solitary gesture recognition framework, it utilizes right-handed gesture signals, and it is characterized and perceived for the particular character. Static gesture recognition framework is proposed which does not require any color code. The sign acknowledgment framework proposed perceives the sign with extraordinary precision and with less features and lesser time. Figure 1 shows the basic methodology steps in recognition of static gestures.

In this paper, we presented our project with five sections. Section 1 is complete literature survey and introduction. Section 2 explained about the process of methodology steps in recognition of gestures with image transformation [6]. Section 3 explained about involved algorithms for our project and some related program segments. Section 4 explained about implementation of project with some related test cases. Finally, we concluded the project with our contribution and future work.

Fig. 1 Methodology for static hand gestures



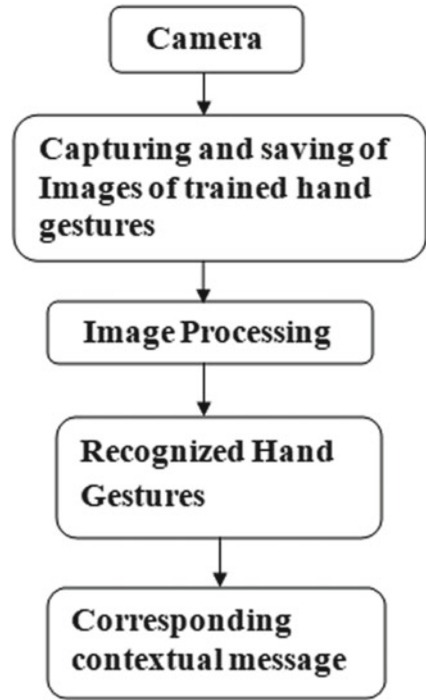
2 Literature Survey

Our model is developed based on the static had gestures recognition system. The static hand gesture system basically follows the four steps. They are pre-processing and segmentation, feature extractions, classification and bit generation, and hand gesture interpretation [7, 8]. For our project, we have prepared the set of input images for each sign which may have slight difference with each other but prepared for same sign. When the camera scans the image of sign as input to the system, application starts the comparisons with stirred dataset. In this model, the hand movements also called gestures are identified by using a camera. After that, these images are sent to next level processing system called image processing to provide the output for given gesture. Figure 2 shows the basic steps involved in processing of hand gestures recognition.

Retrieving of image from saved database and applying the gray code conversion are one of the important processes in the algorithm. Initially, the captured gesture will be saved as an image. These saved images are retrieved from the dialog box. The image which is selected from dialog box is sent for gray-scale conversion process which means the 24-bit pixel image is converted into 8-bit pixel image.

The RGB color values should be converted into gray-scale values by forming a weighted sum of the *R*, *G*, and *B* components based on this formula: $Gray = 0.2989 * R + 0.5870 * G + 0.1140 * B$. The RGB formatted image is converted into gray-coded image, and then, gray-coded image is converted into binary image. In this process, Pixel Count Algorithm recommended using MATLAB function `im2`. The binary image consists of only two values; they are 0 and 1. White pixels are represented by 1, and black pixels are represented by 0. The medium value is 0.5 which is used to help in identifying the skin pixels and background pixels [9–11].

Fig. 2 Basic steps for static hand gesture recognition process



2.1 Morphological Operations

To identify the correct gesture, here we are applying morphological operation which erodes and dilates the image. Erosion removes the finger part dots or pixels. Dilation is used to filter the image after the finger part is removed. This process separates the hand part and finger parts. Basic formulas for erosion and dilation are as follows:

Erosion:

$$(A \ominus B)(x, y) = \min\{A(x + x', y + y') - B(x', y') | (x', y') \in DB\} \quad (1)$$

Dilation:

$$(A \oplus B)(x, y) = \max\{A(x - x', y - y') - B(x', y') | (x', y') \in DB\} \quad (2)$$

where image is represented by A; in this process, structured elements are represented by B; and D indicates the domain. Figure 3 shows the complete processing steps in the recognition of hand gesture from camera image to final signal output.

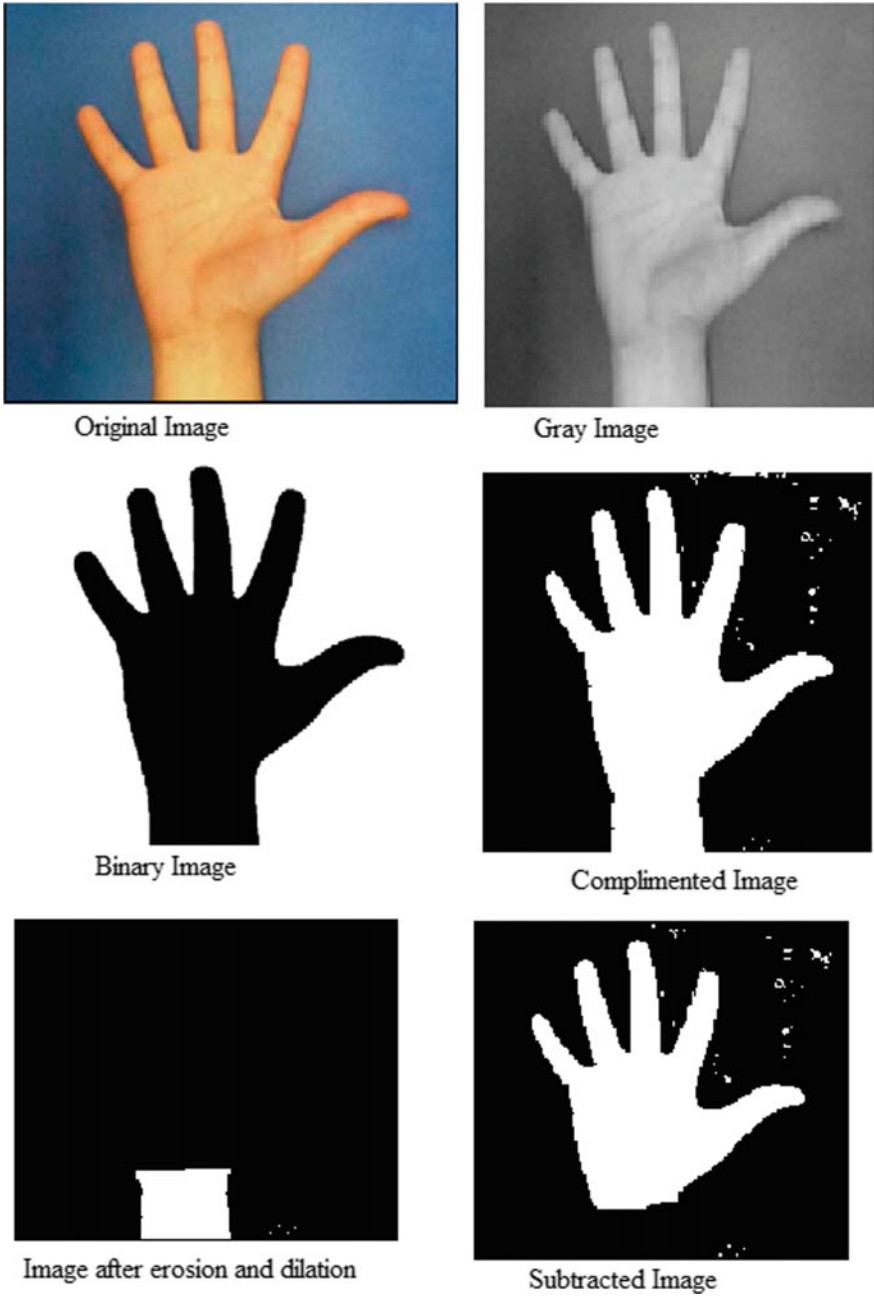


Fig. 3 Complete processing steps of hand gestures

We need to identify only sign covered part of the hand; only remaining part should be eliminated. So that we need to select the complimented image which is a binary-coded image from that subtract the image who applied with erosion and dilation operation.

Subtracted image = Binary image – Image after morphological operations.

2.2 Feature Extraction

We present the gestures in different shapes. These shapes are detected by feature extraction methods. In this procedure, some redundant pixels like some shadows get removed and also the white dots below the threshold are removed. Finally, it keeps the refined suitable part of the image.

2.3 Edge Detection

Hand gestures are represented with only fingers. We need to identify the proper hedge part of the fingers to extract it. For this process, in our project, we implemented the Canny edge detection method. This algorithm is more efficient because it will not be effected by any kinds of unnecessary noise and detect the exact true values. In this Canny edge detection, several processing steps are there to execute the model; they are smoothing the image of hand gesture with Gaussian filter, identifying intensity gradients, suppression, double threshold, and edge tracking. Smoothing the image of hand gesture with Gaussian filter is defined as [12]:

$$H_{ij} = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{(i - (k + 1))^2 + (j - (k + 1))^2}{2\sigma^2}\right) \quad (3)$$

Here, i, j values defined as $1 \leq i, j \leq (2k + 1)$. The kernel size of filter will be $(2k + 1) \times (2k + 1)$.

To find the intensity gradients as given below:

$$G = \sqrt{G_x^2 + G_y^2} \quad (4)$$

$$\Theta = a \tan 2(G_y, G_x) \quad (5)$$

3 Algorithms with MATLAB for Gestures

Our application is integrated with many technologies and algorithms. We need to apply the image processing to identify the proper comparisons with features, filter the data and convert into binary format, classification among the related images, clustering and etc. Different kind of algorithms and their related code parts are included with our project in the MATLAB. There are some primitive methods, procedure, and variables that are available in the MATLAB to perform the above mentioned operations.

3.1 Principal Component Analysis (PCA)

PCA may be a statistical method to find the orthogonal transformation. The PCA also presents the pool of correlated observed data variables into a pool of metrics of linearly uncorrelated variables. Here, the uncorrelated items are also called as principal components. This change is clarified in such how that the essential head part has the most significant conceivable fluctuation and each succeeding segment will have the absolute best difference conceivable under the imperative that it is symmetrical to the former segments [13, 14]. The output vectors are an uncorrelated orthogonal basis set. PCA is sensitive with reference to the relative scaling of the first variables.

Principle component analysis (PCA) is used to calculate the Fisher linear discriminate (FLD) features to evaluate the most discriminating features between images. In our project, we have implemented in the MATLAB with PCA base primitive procedures and commands to process the images.

```

Code segment of PCA in MATLAB:
Train image
[PCAfeatures omega] = PCATraining(ImgMat,nRows,nColumns,ShowOutput,nEigValThres);
[V_FisherProjectedImages_Fisher] =
ASL.fisher(ImgMat,PCAfeatures,nRows,nColumns,omega,size(cAlpha,2),nTrainingSamples,ShowOu tput);
%%Test Classifier StartImage = 1;
EndImage = 5;
NoOfImage = EndImage - StartImage - 1;
PCACorrect_SVM = zeros(size(cAlpha,2),1);
PCACorrect_KNN = zeros(size(cAlpha,2),1);
LDACorrect_SVM = zeros(size(cAlpha,2),1);
LDACorrect_KNN = zeros(size(cAlpha,2),1);
for ii = 1:size(cAlpha,2)
forjj = StartImage:EndImage
%% Input Image
InputImage=strcat(cAlpha(ii),'-test',int2str(jj),'.jpg');%Formfilename
img1 =imread(char(InputImage));%% Perform preprocessing of input image
Proclmg = preprocessing(img1,nRows,nColumns,threshold,ShowOutput);
InImWeight = PCAget(double(Proclmg),PCAfeatures);
InImWeight2 = Fisherget(double(Proclmg),PCAfeatures,V_Fisher)
    
```

3.2 Linear Discriminant Analysis (LDA)

LDA is a speculation of Fisher's linear discriminate. This LDA needs to be evaluated on pattern recognition and linear combinations in AI and isolates at least two classes of objects or events [15]. LDA is additionally firmly identified with PCA that the two of them identify the linear combinations of variables.

```
Code segment for LDA in MATLAB:
LDACorrect_SVM = zeros(size(cAlpha,2),1);
LDACorrect_KNN = zeros(size(cAlpha,2),1);
total_images=size(cAlpha,2)*NoOfImage;
display('Percentage PCA SVM correct-'); sum(PCACorrect_SVM)/total_imagesdisplay('Percentage PCA KNN
correct-'); sum(PCACorrect_KNN)/total_images display('Percentage LDA SVM correct-');
sum(LDACorrect_SVM)/total_images display('Percentage LDA KNN correct-');
```

3.3 K-Nearest Neighbors Algorithm (k-NN)

In this model to classification and regression of input gestures in the way of pattern recognition implemented with k-Nearest Neighbor's algorithm. Here, the k number of training data contains to find feature set. To derive the output in the MATLAB tool available with set of classes.

```
Code segment for k-NN in the MATLAB:
This function performs KNN classification
functionClass=ASlknn(cAlpha,nTrainingSamples,InImWeight,omega)% This function performs KNN
classification
Class = fitcknn(InImWeight, Training, Group, nTrainingSamples, 'euclidean','random');
%Performknn classification with Euclidean norm as basis
Perform KNN and SVM classification
Class=ASlknn(cAlpha,nTrainingSamples,InImWeight,omega);
Ind=ASLsvm(cAlpha,nTrainingSamples,InImWeight,omega);
Class2 = ASlknn(cAlpha,nTrainingSamples,InImWeight2',ProjectedImages_Fisher);
Ind2 = ASLsvm(cAlpha,nTrainingSamples,InImWeight2',ProjectedImages_Fisher);
Display Input and Matched Output f = figure();
set(gca, 'fontsize', 28);
set(f,'name','KNN') subplot (1,3,1) imshow(img1);
title('Input image','fontsize', 20)
subplot (1,3,2)
RecongImg = strcat(cAlpha(Class),'-test1.jpg');
imshow(char(RecongImg));
title(strcat('RecognizedLetterusingPCA-',cAlpha(Class)),'fontsize',20);
subplot(1,3,3)
RecongImg = strcat(cAlpha(Class2),'-test1.jpg');
imshow(char(RecongImg));
title(strcat('RecognizedLetterusingFLD-',cAlpha(Class2)),'fontsize',20);
f =figure();
set(gca, 'fontsize', 28);
set(f,'name','SVM') subplot (1,3,1) imshow(img1);
title('Input image','fontsize', 20)
subplot (1,3,2)
RecongImg = strcat(cAlpha(Ind),'-test1.jpg');
imshow(char(RecongImg));
title(strcat('RecognizedLetterusingPCA-',cAlpha(Ind)),'fontsize',20);
subplot(1,3,3)
RecongImg = strcat(cAlpha(Ind2),'-test1.jpg');
imshow(char(RecongImg));
title(strcat('Recognized Letter using FLD-',cAlpha(Ind2)),'fontsize', 20);
```

3.4 Support Vector Machine (SVM)

A support vector machine is a classification algorithm under category of supervised learning based and that sorts information into two classes [15, 16]. This makes SVM a sort of non-double straight classifier. A SVM calculation ought to put objects into classes. However have the edges between them on a chart as wide as could reasonably be expected. A few utilizations of SVM include the following:

- Text and hypertext characterization
- Image characterization
- Recognizing manually written characters
- Biological sciences, including protein characterization

Code segment of SVM in the MATLAB:

```
function Ind = ASLsvm(cAlpha,nTrainingSamples,InImWeight,omega) % This
function performs SVM classification.

Training = omega';%Training based on features extracted.

%SVM.

Ind = 1;

for ii = 2:size(cAlpha,2).

Group = [ii*ones(1,nTrainingSamples) Ind*ones(1,nTrainingSamples)];

%Perform classification between chosen and next group of training.

%samples.

Train = [Training((ii-1)*nTrainingSamples + 1:(ii-1)*nTrainingSamples + nTrain-
ingSamples,:); Training((Ind-1)*nTrainingSamples + 1:(Ind-1)*nTrainingSamples
+ nTrainingSamples,:)]; SVMStruct = svmtrain(Train, Group);

Ind = svmclassify(SVMStruct,InImWeight);%Chosengroupretainedfornextcomparison.

end.
```

4 Implementation

The input picture can be captured utilizing with web cam. The pictures caught have their specified position with support format of the device. The format which is supported by the device of web cam can be identified by a command which initializes the order: 'imaqhwinfo('winvideo').' This order gives the subtleties, for example, AdaptorDllName: [1 × 81 char] AdaptorDllVersion: '4.5 (R2013a)' AdaptorName: 'winvideo' DeviceIDs: DeviceInfo: [1 × 1 struct]. With the utilization of device ID, we can get the upheld group by the web cam for the picture. The caught picture ought



Fig. 4 Sample train images of character C

to be resized to the size of the put away pictures of the informational collection. In this way, grid of the pictures is of same estimate and can be utilized for numerical count of Euclidean distance. Figure 4 shows the collected trained data sent to recognize the character C by using hand gesture. Figure 5 shows the collected trained dataset to recognize the character 5 by using hand signature in different angles.

4.1 Pre-processing and Segmentation

Pre-processing is required on every picture which is captured by camera to improve the usefulness of picture preparing for gesture. Image processing needs to identify the different objects with respect to feature set. As we discussed previously, image subtraction, pre-processing, RGB to gray conversion, and segmentation are done in the first stage [17, 18]. The segmentation process portions the picture into two shades, one is foundation, and other one is closer view with district of intrigue that is hand locale. The portioned picture has the hand area with the pixel esteem '1' and the foundation as the '0.' This picture is then utilized as a veil to get the hand area from the RGB picture by duplicating the highly contrasting picture, for example, paired picture with the first RGB picture, plane via plane. The size of picture is resized to decrease size of the network, utilized for the acknowledgment procedure.

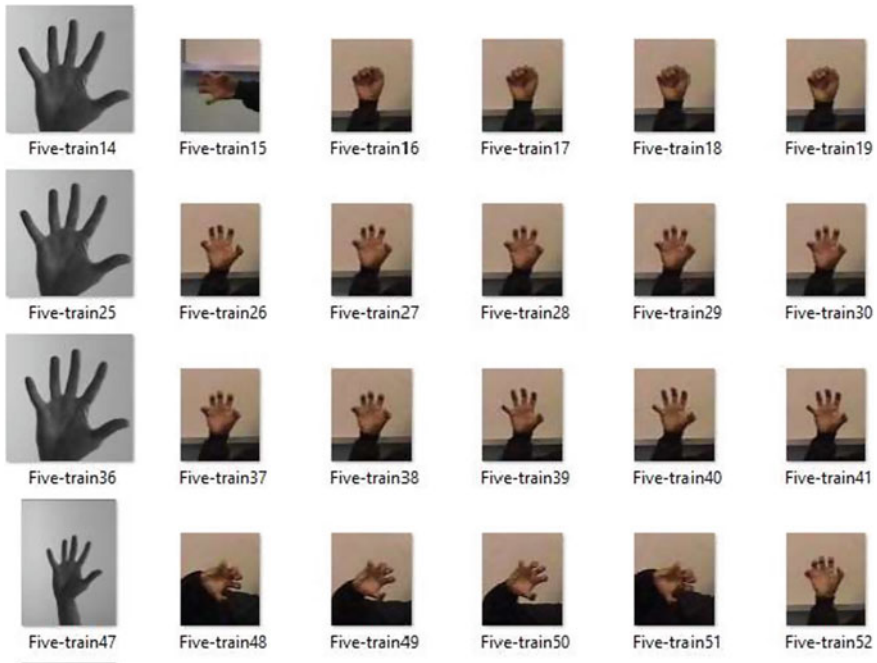


Fig. 5 Sample train images of character 5

4.2 Feature Extraction and Training Phase

Feature extraction is one of the important steps in the gesture identification. In this process, the features are retrieved by using PCA technique and the hand region properly cropped with respect to signature of the character [19]. The subtraction of the image and normalization are the subsequent processes as we discussed in earlier.

In this, the preparation set for the framework to perceive the predefined gesture is finished. During the age of the preparation set, the pictures are pre-processed and afterward put away. Column matrix is inferred for every one of the picture of dataset [9]. Utilizing that column matrix, Eigen vector is determined. Eigen vector matrix is then increased with every one of the section vector framed by the dataset pictures. Finally, optimal hand gesture will be recognized.

4.3 Test Cases

In the test cases, the character C, A, and 5 are presented for sample outputs. Accordingly, they are available with all possible trained dataset with different angles. Figure 6 shows the test case for character C, Fig. 7 shows the test case for hand gesture A, and Fig. 8 shows the test case output for symbol 5.

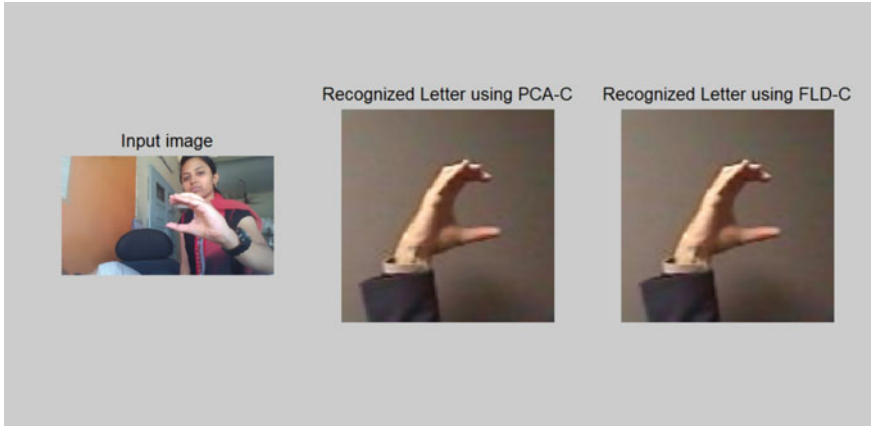


Fig. 6 Test case for character C

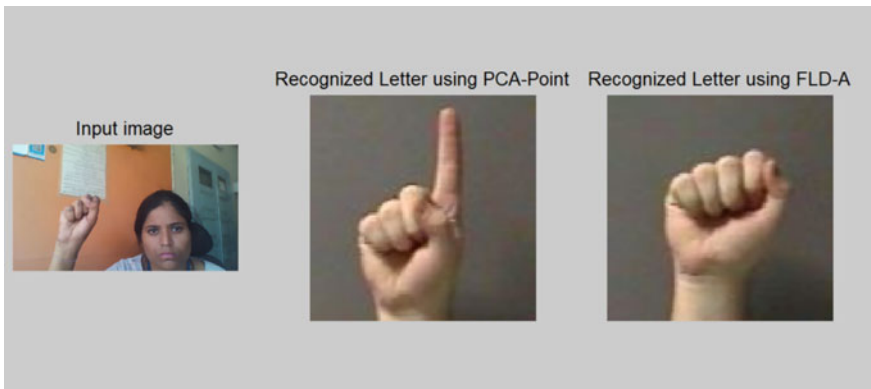


Fig. 7 Test case for character A

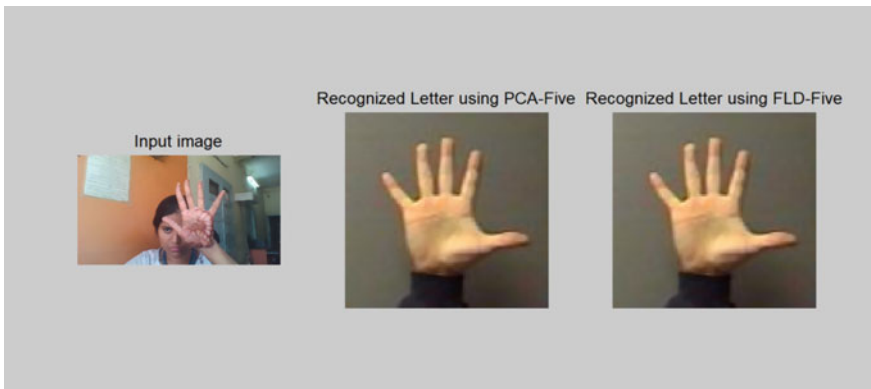


Fig. 8 Test case for character 5

5 Conclusion

Almost deaf and discourse disabled people utilize gesture-based communication to impart. This framework application is to give a stage high precision to decipher the signs, empowering typical individual to get motion. The distinguished or perceived character can be shown just as articulated. Gesture recognition framework utilizing PCA method is created, and it keeps up precision, for example, with different frameworks or executed methods. Quiet mute and hard of hearing people need translators to communicate to avoid the third person help. This system is more helpful to the persons who are old aged deaf and dumb persons to communicate easily with society. However, gesture recognition system needs more research and defines easy way to communicate with the people for physical defected people. In future, I will continue my research in this area to resolve the complication in the gesture recognition system.

References

1. Pillai A, Sinha S, Das P, Chanu OR (2017) Contrivance of recognised hand gestures into voice and text output. In: Proceedings of 35th IRF international conference, pp 41–45
2. Motoche C, Benalcázar ME (2018) Real-time hand gesture recognition based on electromyographic signals and artificial neural networks. In: International conference on artificial neural networks, pp 352–361
3. Subbarao MV, Terlapu SK, Chakravarthy VVSSS, Satapaty SC (2021) Pattern recognition of time-varying signals using ensemble classifiers. *Microelectronics Electromagnetics and Telecommunications*. Springer, Singapore, pp 725–733
4. Praveen P, Rama B (2018) A novel approach to improve the performance of divisive clustering-BST. In: Satapathy S, Bhateja V, Raju K, Janakiramaiah B (eds) *Data engineering and intelligent computing. Advances in Intelligent Systems and Computing*, vol 542. Springer, Singapore
5. Pappula P, Rama B, Javvaji R (2014) Experimental survey on data mining techniques for association rule mining. In: *International journal of advanced research in computer science and software engineering*
6. Sheshikala M, Rao DR, Prakash RV (2017) a map-reduce framework for finding clusters of colocation patterns-A summary of results. In: 2017 IEEE 7th international advance computing conference (IACC), pp 129–131
7. Shaik MA, Praveen P, Prakash DR (2019) Novel classification scheme for multi agents. *Asian J Comput Sci Technol* 8(S3): 54–58, ISSN 2249-0701
8. Kothandaraman D, Sheshikala M, SeenaNaik K, Chanti Y, Vijyakumar B (2019) Design of an optimized multicast routing algorithm for internet of things. *Int J Recent Technol Eng (IJRTE)* 8(2)
9. Kumar RR, Reddy MB, Praveen P (2017) A review of feature subset selection on unsupervised learning. In: *IEEE conference, 3rd international conferences on advances in electrical, electronics, information, communication and bio-informatics (AEEICB17)*
10. Kumar RR, Reddy MB, Praveen P (2019) Text classification performance analysis on machine learning. *Int J Adv Sci Technol (IJAST)* 28(20):691–697
11. Mohmmad S, Sheshikala M, Shabana (2018) Software defined security (SDSec): reliable centralized security system to decentralized applications in SDN and their challenges. *J Adv Res Dyn Control Syst* 10(10):147-152
12. Chanu OR, Pillai A, Sinha S, Das P (2017) Comparative study for vision based and data based hand gesture recognition technique. *Int Conf Intell Commun Comput Tech (ICCT) 2017:26–31*. <https://doi.org/10.1109/INTELCCT.2017.8324015>

13. Joshi A, Monnier C, Betke M, Sclaroff S (2017) Comparing random forest approaches to segmenting and classifying gestures. *Image Vis Comput* 58:86–95
14. Zhang Y, Cao C, Cheng J, Lu H (2018) Egogesture: a new dataset and benchmark for egocentric hand gesture recognition. *IEEE Trans Multimedia* 20:1038–1050
15. Coteallard U, Fall CL, Drouin A, Campeulecours A, Gosselin C, Glette K, Laviolette F, Gosselin B (2019) Deep learning for electromyographic hand gesture signal classification using transfer learning. *IEEE Trans Neural Syst Rehabil Eng* 27:760–771
16. Rekha J, Bhattacharya J, Majumder S (2011) Shape, Texture and local movement hand gesture features for Indian sign language recognition. *IEEE*
17. Xu Y, Dai Y (2017) Review of hand gesture recognition study and application. *Contemp Eng Sci* 10:375–384
18. Mizuno H, Tsujiuchi N, Koizumi T (2011) Forearm motion discrimination technique using real-time EMG signals. In: 2011 Annual international conference of the IEEE, Engineering in Medicine and Biology Society, EMBC, pp 4435–4438
19. Kumar RR, Reddy MB, Praveen P (2019) An evaluation of feature selection algorithms in machine learning. *Int J Sci Technol Res (IJSTR)* 8(12):2071–2074

Emotion Recognition Based on Streaming Real-Time Video with Deep Learning Approach



M. Sheshikala, Sallauddin Mohmmad, D. Kothandaraman, Dadi Ramesh, and Ranganath Kanakam

Abstract Emotion recognition has gained a lot of traction lately. It is also a very fast growing field with a huge amount of investment and research going into it. In this paper, we discuss video-based emotion recognition made possible by deep learning. Although there are many methodologies on how to do video-based emotion recognition, there is a need for comprehensive methodology where it ends with deployment. We are using the FER2013 Kaggle Challenge dataset. It is a collection of pixel data of human face images in grayscale with 48×48 as dimensions. The emotion categories included in the dataset are Angry, Disgust, Fear, Happy, Sad, Surprise, and Neutral. The model training using deep learning and flask is used for the deployment. The main objective would also be to bring forth an open source methodology that can be used for many applications irrespective of the domain.

Keywords Emotion recognition · Deployment · Deep learning

1 Introduction

The importance of emotion recognition is very crucial for a proper interaction between machines and humans and the effective development would lead to an increased trust factor. Emotion recognition is being used for various applications like driver fatigue prediction [1], designing responsible robots [2], and also during candidate proctoring and testing in online exams and interviews.

It is often hard to predict the emotion of a human as it is not defined by a specific set of parameters all the time and it varies from person to person [3, 4]. Initially, the source of emotion recognition was audios and images with clear distinct facial expressions

M. Sheshikala (✉) · S. Mohmmad · D. Kothandaraman · D. Ramesh
School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India
e-mail: marthakala08@gmail.com

R. Kanakam
Department of Computer Science and Engineering, Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India

were used but the introduction of deep neural networks has been very helpful in overcoming the limitations and thereby marking the start for various implementations that can now extract patterns/features that were impossible to be made use of before [5, 6].

Whenever facial emotion recognition is considered a good start to explore the convolutional neural networks (CNNs) as these provide a good foundation on how to implement the proposed methodology [7–9]. The ever increasing complexity of these networks is allowing them to decode even toughest of the recognition tasks of the open world [19, 20].

2 Data Description

The dataset taken under consideration is the FER2013 dataset, upon exploring, it is evident that the data is imbalanced and this has a potential to affect the result badly. The train set has 28,709 images, the test set has 3589 images. For each image, the dataset contains the grayscale color of 2304 pixels (48×48), as well as the emotion associated. We can then take a look at the important regions of the image when it comes to classification tasks. From Fig. 1, we can comprehend the manner in which an emotion is being deciphered inside the data. It is evident that the eye axis for anger is not quite the same as that of happiness [1].

3 Approach

Minimizing overfitting is one of the key challenges that need to be addressed. In reality, because of the huge class irregularity and parameter number that should be learnt, the models can undoubtedly overfit [10–12]. This is the reason behind implementing methodologies and strategies that have been created and developed. In the coming sections, we will cover the fundamental strategies and the results of these various methods along with the implementation of the finalized model [13].

3.1 Using Auto-Encoders for Dimensionality Reduction

Firstly, dimension reduction is done by auto-encoding the images in the data. Based on the proposal of the auto-encoder, the input image dimensions were reduced to 12×12 pixels which is a 95% reduction to the original image's dimensions. This amount of reduction results in a huge loss of information as the risk of not being able to completely understand the key features is high.

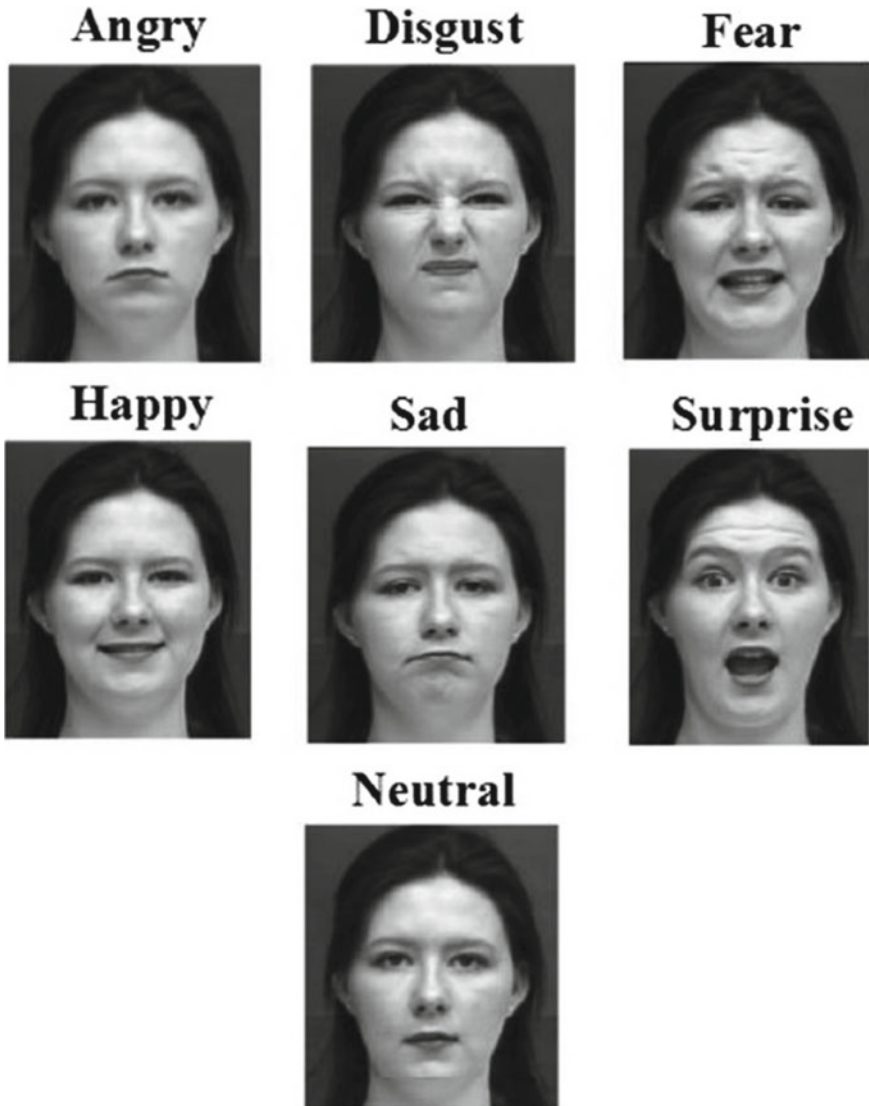


Fig. 1 Emotion of averaged faces [1]

3.2 Model Used—Xception

We have used the Xception model which is a convolution neural network algorithm. CNN is expressed as a multilayer perceptron that is used to identify an image formation. The architecture typically contains: input layer, hidden layer(s), and an output layer [14, 15]. These layers have neurons that are very crucial for updating weights

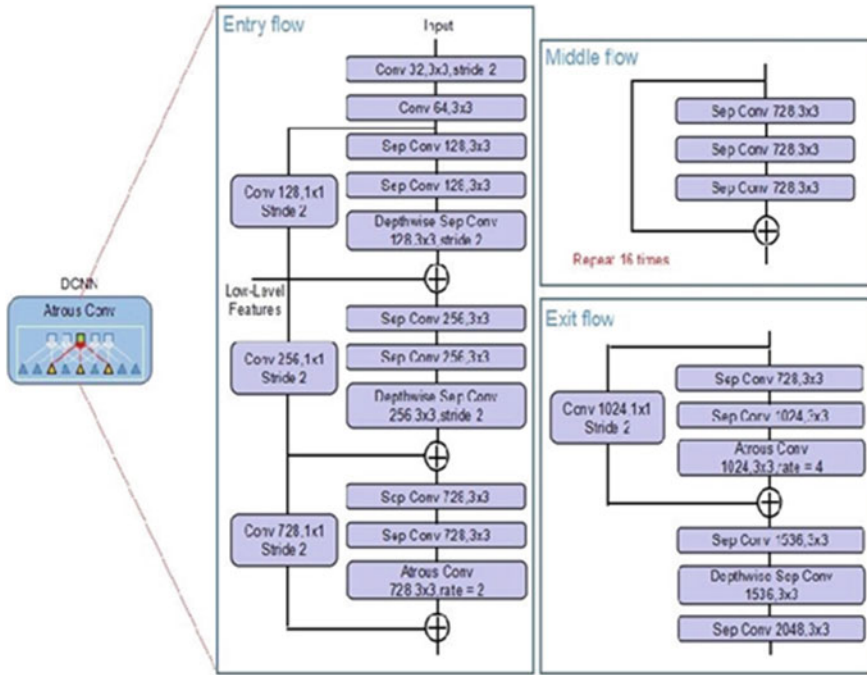


Fig. 2 Architecture of Xception

and improving the training. CNN has come into existence having image training as the primary target but now it is being extended to various other applications and is proving revolutionary [16].

Xception, developed by Google researchers, is a deep convolutional neural network. It includes depth wise separable convolutions which can be comprehended as an inception module coupled with a huge number of towers [17, 18]. The observation of this kind made by the researchers had paved the way for the design of a new model formed by replacing the modules in the inception model by depth wise separable convolutions. The data flow can be described from Fig. 2 where initially the data flows through entry flow, followed by middle flow, and then the exit flow. Batch normalization follows each and every layer included in the architecture.

3.3 Implementation Process

Analyzing emotion from a video is obviously more meticulous when compared to emotion extraction from an image. The following steps are used for predicting the emotion from a video stream of a Webcam: image by image breakdown of the video, zoom the identified image, dealing with multiple images (if present), bringing down,

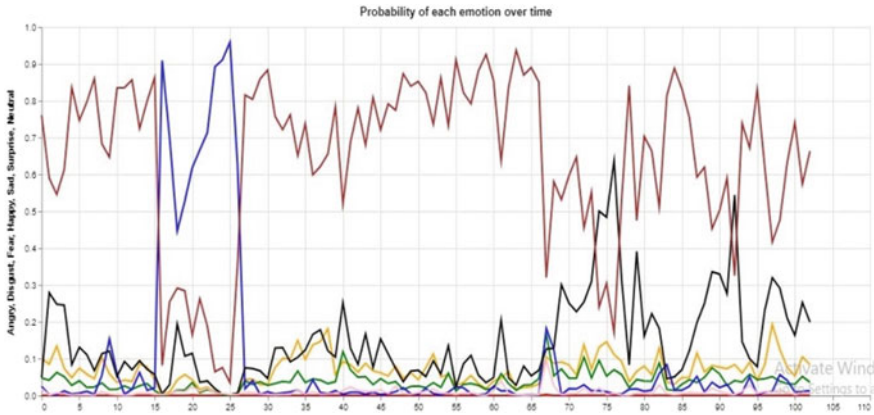


Fig. 3 Emotion graph for all labels over time

the pixel density to match the pixel density of the images in the training set, using the model to predict the emotion of the image.

The OpenCV package of python is used for image processing and cascade classifier is used for detection of faces. For face detection, pre-trained cascade models are made available by OpenCV. Emotion classification using a Webcam and deciding model is working fine but there is scope of a lot of improvement.

We had made use of flask for the deployment of the model onto the Web site. The Web site makes use of the Webcam present on the device to capture the input and thereby giving the output on to another page of the Web site. Figure 3 shows the emotion graph for all labels over the time.

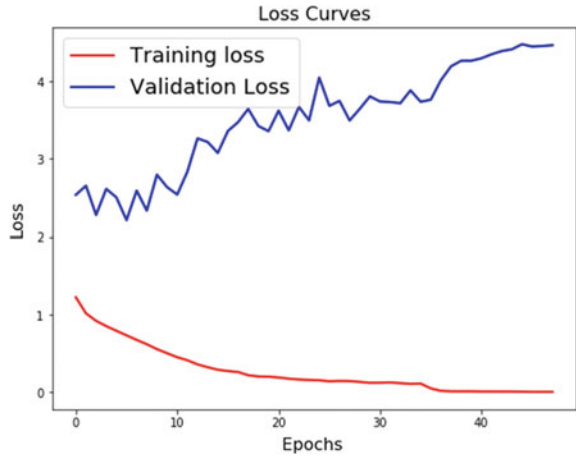
4 Results

The model we used for the final implementation was Xception and we also used VGG16, VGG19, and DenseNet. The Xception model was the clear winner in terms of accuracy among all the models considered in Table 1.

Table 1 Different models with accuracy

Model	Accuracy (in %)
VGG16	46
VGG19	51
DenseNet	53
Xception	54

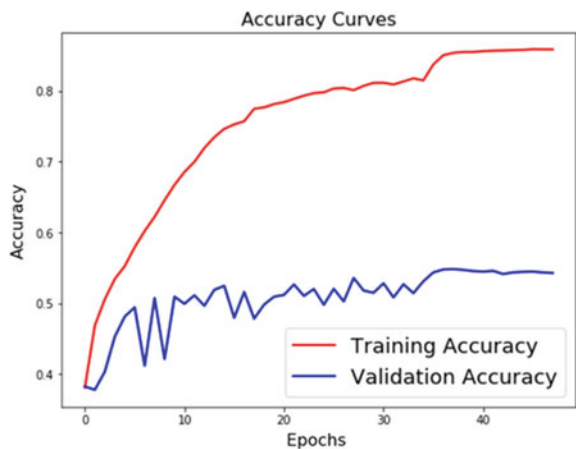
Fig. 4 Loss before image augmentation



The loss and accuracy graphs of the Xception model are as follows. Figure 4 shows the resultant graph of loss before image augmentation. Figure 5 shows the resultant graph of accuracy before image augmentation.

Since the performance is not **commend**ing, we implemented image augmentation to improve the performance of the model. Image augmentation is created to generate alternate images from a current dataset. Image augmentation is the way toward taking pictures that are as of now in a preparation dataset and manipulating them to make many adjusted adaptations of a similar picture. This gives more pictures for training; however, can likewise help open our classifier to a more extensive assortment of lighting and shading circumstances to make our classifier more powerful. For image augmentation, we have made use of the ImageDataGenerator class from Keras. The attributes we made of use to generate the data are as follows:

Fig. 5 Accuracy before image augmentation



- zoom_range, used to zoom into existing images randomly.
- rotation_range, used to rotate image based on the angle mentioned from 0 to 180.
- width_shift_range, used to shift images horizontally randomly.
- height_shift_range, used to shift images vertically randomly.
- horizontal_flip, flip images randomly.

The loss and accuracy trends after using the Xception model on the data including augmented images. Figure 6 shows the resultant of loss after image augmentation and Fig. 7 shows the accuracy after image augmentation. The final accuracy was nearing 64% and was decent for us to proceed about the implementation result.

Fig. 6 Loss after image augmentation

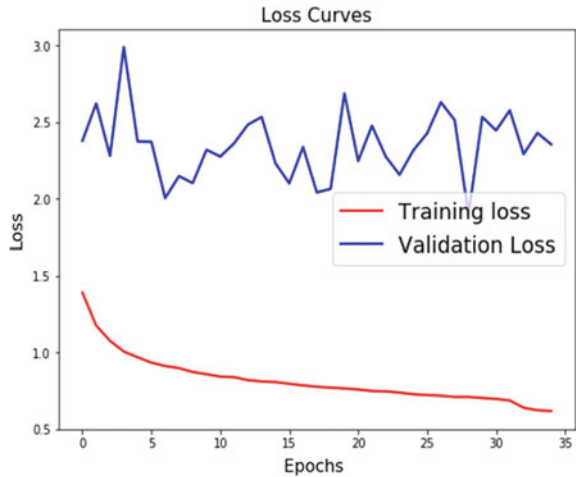
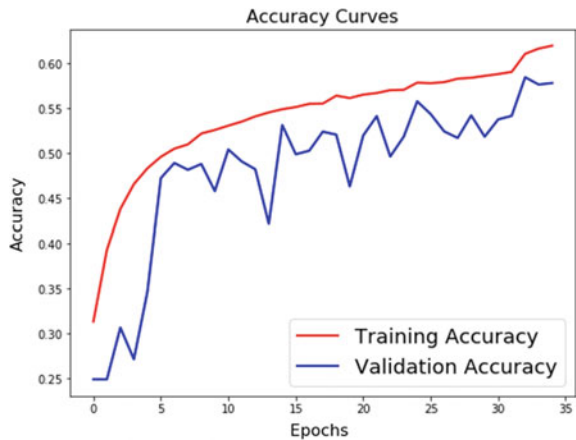


Fig. 7 Accuracy after image augmentation



5 Conclusions

In terms of research and implementation that follows all the discussed work in this paper, we would expand to multimodal emotion recognition. Although we had used the model with various tunings and improvements in terms of image augmentation, there is still scope for improvement. Exploring and making use of the updated and also huge datasets will certainly make the model improvement and in turn result in better outcomes. Essentially, its emotion recognition from text, audio, and video formats. We are planning to design a common platform for the entire multimodal emotion recognition which can be used for various purposes and also for drawing insights that can be used across the different methods.

References

1. Fan Y, Xiangju L, Dian L, Yuanliu L (2016) Video-based emotion recognition using CNN-RNN and C3D hybrid networks. In: Proceedings of the 18th ACM international conference on multimodal interaction, pp 445–450
2. Kaya H, Furkan G, Albert Ali S (2017) Video-based emotion recognition in the wild using deep transfer learning and score fusion. *Image Vis Comput* 65:66–75
3. Fan Y, Lam JC, Li VO (2018) Video-based emotion recognition using deeply-supervised neural networks. In: Proceedings of the 20th ACM international conference on multimodal interaction, pp 584–588
4. Dhall A, Ramana Murthy OV, Goecke, R, Joshi J, Gedeon T (2015) Video and image based emotion recognition challenges in the wild: emotiw 2015. In: Proceedings of the 2015 ACM on international conference on multimodal interaction, pp 423–426
5. Gunawan TS, Ashraf A, Riza BS, Haryanto EV, Rosnelly R, Kartiwi M, Janin Z (2020) Development of video-based emotion recognition using deep learning with Google Colab. *TELKOMNIKA* 18(5):2463–2471
6. Liu C, Tang T, Lv K, Wang M (2018) Multi-feature based emotion recognition for video clips. In: Proceedings of the 20th ACM international conference on multimodal interaction, pp 630–634
7. Mohammad S, Rao DS (2021) Preserving the forest natural resources by machine learning intelligence. In: International conference on intelligent and smart computing in data analytics: ISDA 2020. Springer, Singapore, pp 239–253
8. Kumar PP, Kumar SN, Thirupathi V, Sandeep C (2019) QOS and security problems in 4G networks and QOS mechanisms offered by 4G. *Int J Adv Sci Technol* 28(20):600–606
9. Kumar BV, Chanti Y, Yamsani N, Aluvala S, Bhaskar B (2019) Design a cost optimum for 5G mobile cellular network footing on NFV and SDN. *Int J Recent Technol Eng (IJRTE)* 8(2S3) ISSN 2277-3878
10. Sallauddin M, Sheshikala M (2018) Software defined security (SDSec): reliable centralized security system to decentralized applications in SDN and their challenges. *J Adv Res Dyn Control Syst* 10(10):147–153
11. Ramesh D, Pasha SN, Sallauddin M (2018) Cognitive-based adaptive path planning for mobile robot in dynamic environment. In: Advances in intelligent systems and computing. Springer, Nov 2018, pp 117–123
12. Shaik MA, Sampath Kumar T, Praveen P, Vijayaprakash R (2019) Research on multi-agent experiment in clustering. *Int J Recent Technol Eng* 8(4):1126–1129

13. Song M, Bu J, Chen C, Li N (2004) Audio-visual based emotion recognition-a new approach. In: Proceedings of the 2004 IEEE computer society conference on computer vision and pattern recognition, 2004. CVPR 2004, vol 2. IEEE, pp II-II
14. Bargal SA, Barsoum E, Ferrer CC, Zhang C (2016) Emotion recognition in the wild from videos using images. In: Proceedings of the 18th ACM international conference on multimodal interaction, pp 433-436
15. Salah AA, Kaya H, Gürpınar F (2019) Video-based emotion recognition in the wild. In: Multimodal behavior analysis in the wild. Academic, pp 369-386
16. Du Z, Wu S, Huang D, Li W, Wang Y (2019) Spatio-temporal encoder-decoder fully convolutional network for video-based dimensional emotion recognition. *IEEE Trans Affect Comput*
17. Sujanaa J, Palanivel S (2020) Real-time video based emotion recognition using convolutional neural network and transfer learning. *Indian J Sci Technol* 13(31):3222-3229
18. Zhou H, Meng D, Zhang Y, Peng X, Du J, Wang K, Qiao Y (2019) Exploring emotion features and fusion strategies for audio-video emotion recognition. In: 2019 International conference on multimodal interaction, pp 562-566
19. Balasundaram A, Kothandaraman D, Kumar PS, Ashokkumar S (2020) An approach to secure capacity optimization in cloud computing using cryptographic hash function and data duplication. In: 2020 3rd international conference on intelligent sustainable systems (ICISS), pp 1256-1262
20. Harshavardhan A, Ramesh D, Pasha SN, Shwetha S, Mohmmad S, Kothandaraman D (2020) Lifting wheelchair for limbless people. *IOP Conf Ser Mater Sci Eng* 981(2):022036

Efficient Dynamic Framework to Secure MQTT to Detect Distributed DoS Using Meta-Empirical Clustering



V. Thirupathi and K. Sagar

Abstract The development of IoT plays a significant role for the development of new wireless communication. As Message Queuing Telemetry Transport (MQTT) with certain constraints helps to make IoT operations to complete based on Machine-to-Machine (M2M) communication. For MQTT, security is a crucial factor when there is a communication establishment due to the increase in the usage of IoT devices and there is a need to secure the communication. There is a possibility of various attacks like Denial of Service (DoS) and Distributed Denial of Service (Distributed DoS) whenever IoT communication is open one, and there are several IoT applications like health monitoring, smart home, etc. while considering the attack of DoS and Distributed DoS, effective intrusion detection system (IDS) is needed by considering the IoT-based application. In this work, we have proposed the optimization mechanism based on meta-empirical clustering for Distributed DoS detection to mitigate the DoS and Distributed DoS attacks based on the attack request. The effective mechanism helps to secure the MQTT and detect the malicious behaviour of the nodes in the network. The performance analysis to be done as to show the proposed method gives more accuracy compared to existing ones such as MQTT security and CoAP and XMPP.

Keywords MQTT · IDS · DoS · DDoS

1 Introduction

In recent days, IoT plays a significant role while establishing communication for heterogenous devices as the number of IoT devices will increase drastically in 2021. When the communication is established among numerous IoT devices [1], it is very

V. Thirupathi (✉)
Department of CSE, SR University, Warangal, Telangana, India
e-mail: v.thirupathi@sru.edu.in

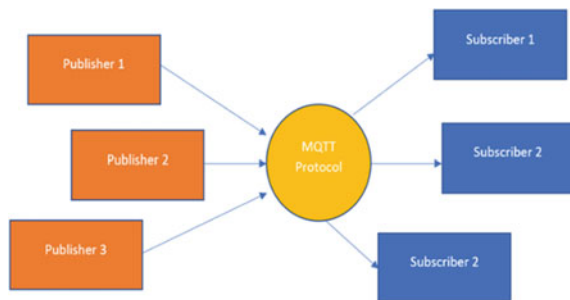
K. Sagar
Department of CSE, CBIT, Hyderabad, Telangana, India

complex to manage the data, which are transferred and there may be a chance of intrusion attack problem. To transfer the message in IoT communication [2], there are several existing protocols available such as Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP) and Advanced Message Queuing Protocol (AMQP).

From the above protocols, MQTT is much light weight protocol and performs low-power consumer with more work effectiveness [3]. When the MQTT is added up with IoT, it will provide multiple services to the user devices. As in recent days, humans have limited amount of time and need of machine, which can able to fulfil the different aspects of life. The machine that is used should be programmed automatically and executed. In October 2016, Distributed DoS (Distributed Denial of Service) attack has been made in botnet device in syn DNS and followed by several similar instance has been happened by Distributed DoS attack. As IoT devices are robust in nature and no ensure of security whenever it is in danger to provide effective security. As we know, the IoT devices are growing enormously and increasing day by day and these mobile devices are used in various applications where the vast feature of user satisfaction and user services are provided. In recent days, these IoT devices are added to provide features like supporting advanced wireless technologies, seamless mobile connectivity and improved processor speed and ensure security protection. This security in IoT devices helps the service provider to satisfy the users' satisfaction with improved Quality of Service (QoS). MQTT protocol is developed by IBM, which has the property of light weight communication protocol with the property of machine to machine. This protocol is also a message protocol, and it requires publish-subscribe communication as this protocol makes the clients to have no more updates to reduce the resource usage and makes it optimal in terms of reduced bandwidth.

The MQTT is specific with certain characteristics such as effective QoS (Quality of Service) delivery, bandwidth effectiveness, easy to implement and continuous session. There is a message broker that acts a central hub, which can able to control the messages between the publishers and subscribers as represented in Fig. 1. This protocol functions as a client-server where the broker moves all the updates to MQTT clients, and only based on the broker as the intermediate, clients will send the message to the broker. In this MQTT, messages are sent in the form of tree structure, where client can subscribe or publish. When the broker checks for the message as it is

Fig. 1 Publisher- and subscriber-based MQTT protocol



received from the client, it will be forwarded to all other clients and it can be subscribed to a specific topic.

In this work, modified optimization strategy based on meta-empirical clustering is proposed to secure the MQTT and detect the malicious behaviour of the nodes in the network by mitigating the DoS and Distributed DoS attacks based on effective intrusion detection system. Here, we have applied meta-empirical clustering which helps to identify the network anomalies by the formation of clustering along with the effective IDS system. This proposed strategy helps to maximize the accuracy and protect the entire network from crash.

2 Related Work

In this section, we have discussed the existing works related to IDS algorithms and strategies based on IoT. These algorithms help to avoid the unauthorized access for IoT devices by adding certain conditions in the network. As some standard IDS systems are available such as, group formation, neural as it all categorized based on signature and anomaly-based IDS system. Here, in the discussion of existing IDS systems, we are discussing the system on two system mentioned above.

In the signature-based system, the current behaviour strategy is understood based on the existing IDS strategy they have applied. For the signature based, [4] added two advantages such as easy to implement and low weight and reduced power consuming. By considering the pattern matching, there is a possibility of adding new matching algorithm, which will generate the unique pattern set to improve the efficiency as the future scope. [5] added a proposed pattern matching engine, which uses support moving and decision-making method to increase the efficiency of the IoT devices, and it avoids pattern matching algorithm to increase the computation time. In the anomaly-based system, network activities and their behaviour are observed and supervised during this system. Based on the anomaly system, proposed bottle neck detection system is used to detect the network activities by using the detection module to determine the network traffic of the particular network, which is not yet considered in the standard system discussed before. The bottleneck can be applied by simply sending the spam email and DoS attack, and it can able to negotiate the nodes present in the network. While doing the performance analyses, bottleneck is able to calculate the detection rate but this mechanism fails to discuss the overhead value, while considering the bottleneck detection [6].

After the bottleneck, sink hole detection is proposed [7], which helps to secure the routing process that happens on RPL (Routing Protocol for Low-Power and Lossy Networks) based on IoT (Internet of Things) network. This proposed system helps to detect how many packets are sent and received via network from time to time, and this makes to determine the intrusion rate ratio. While it detects the way in which the positive/negative rate determination takes more energy consumption and it is not suitable for the IoT-based networks [8]. To overcome the problem of energy consumption, authors [9] have proposed the IDS (intrusion detection system) based

on game theory associated with low based constraint devices with IoT network. This proposed system uses Nash equilibrium, which can able to monitor the network activity periodically with reduced energy consumption.

The proposed IDS based on event management for Machine-to-Machine (M2M) networks [10], which focuses on security aspects and apply security into the events with the correlation factor to detect the attacks. The proposed system helps to improve the detection accuracy by adding more security libraries into it.

Now moving on to hybrid IDS [11, 12], which involves both signature and anomaly detection to monitor the network activity and has significant benefits such as improvement towards storage and computational efficiency for both signature and anomaly system. The hybrid strategy is applied for both centralized and distributed approach and associated with low constrained device and router. There may be possibility of going with more attacks based on IoT network. The signature-based system is not able to adopt the continuous data based on heterogenous IoT network [13], to make the approach more effective by applying machine learning concept.

By comparing the signature-based IDS system with anomaly detection system [14], signature will have the detection rate that will be incorrect as the training data cannot take the value of existing events as it is the one of the characteristics. The signature will not be more flexible for continuous steaming of data especially for heterogenous IoT networks. During the detection activity, unconditional activities are not detected effectively but it can be more effective only when it is applied using machine learning techniques.

Thus, the anomaly-based system helps to monitor the network activity when attacked with malicious nodes with MQTT-based IoT network [15]. The MQTT detection has not been effectively considered so far in the above literature. It helps to secure the communication among the IoT devices/applications. It is necessary to add more security into the MQTT as it is more used in the real-time applications like military, health care, smart home, etc. [16]. In this MQTT, IDS is applied with several machine learning algorithms such as genetic, neural network, fuzzy [17], etc., and this learning helps to detect the anomaly that happens in the network. So there needs an IDS system, which will be more effective for IoT network and detection of anomaly users with much easier computation. While differentiating the nonlinear data in uncertainty condition, MQTT has to be proposed by integrating with fuzzy to determine effective computational accuracy [18, 19].

Thus, the existing MQTT is proposed with Secure Session Layer (SSL) and its session can be added with key management and generation, which makes the computation more complex [20]. Here, the proposed MQTT is added with machine learning with fuzzy rule base as it generates the rule in periodical interval of time. So, here the modified optimization strategy based on meta-empirical clustering is proposed to secure the MQTT and detect the malicious behaviour of the nodes in the network by mitigating the DoS and Distributed DoS attacks based on effective intrusion detection system [20].

3 Methodology

To make the anomaly detection, i.e. IDS more effective for IoT device network, MQTT protocol plays a significant role based on application layer while transmitting data via IoT devices in the network. While considering the MQTT, publisher, subscriber and broker are the components used in MQTT to establish a communication between IoT devices. In MQTT, there are certain procedure to be followed to establish the connection by CONNECT and CONNACK message to make the complete connection. Then, the IoT devices use publish and subscribe process to secure MQTT protocol.

So, to make the communication establishment more data scalable and flexible, secure communication exchange among the IoT devices is needed. During the transmission exchange, there may be an anomaly, i.e. intruder will be intruded into the network. So, several existing strategies are proposed, which will be a detection system to monitor the network activity for heterogenous IoT network which will improve efficiency in terms of scalability, throughput, computation time and network complexity. To make it efficient, machine learning process helps to make the network monitoring process more effective. An improved strategy is proposed to monitor and detect the network activity for heterogenous IoT network associated with proposed machine learning approach.

A secure MQTT model is to be proposed, which helps to identify the anomaly/malicious node associated to learning process to monitor and detect the network activity for heterogenous IoT network. To secure the proposed model, some secondary objectives are needed, which are discussed below.

- To design an efficient IDS based on machine learning along with rule-based inference and it helps to select the network traffic with the detection of DoS and Distributed DoS attack.
- To design a modified detection scheme with DoS and Distributed DoS attack by associating the learning algorithm with rule-based inference to update periodically.

Based on the publisher and subscriber protocol, here we have used 'N' no of publisher and subscriber where MQTT is placed in between, which acts as a broker. When there is anomaly happen such as malicious node enters into the network, it gets all the control and these have to be avoided by the broker as it provided multiple service attacker to access to the publisher and subscriber.

The attacker attack the DDoS by sending more connection request to the MQTT broker to make it flooded attack. Here, CONNECT helps only the authenticated request even though there are multiple requests added into the broker, and then, it makes the attacker packet transmission gets delay as it waits for longer time and makes its credentials to be invalid. When the invalid credentials are verified, no authorized access is allowed by the broker to access the topics. MQTT uses TCP to establish the connection as it sends the CONNECT message to the broker and broker will send the acknowledgment by CONNACK. Then, the publisher and subscriber

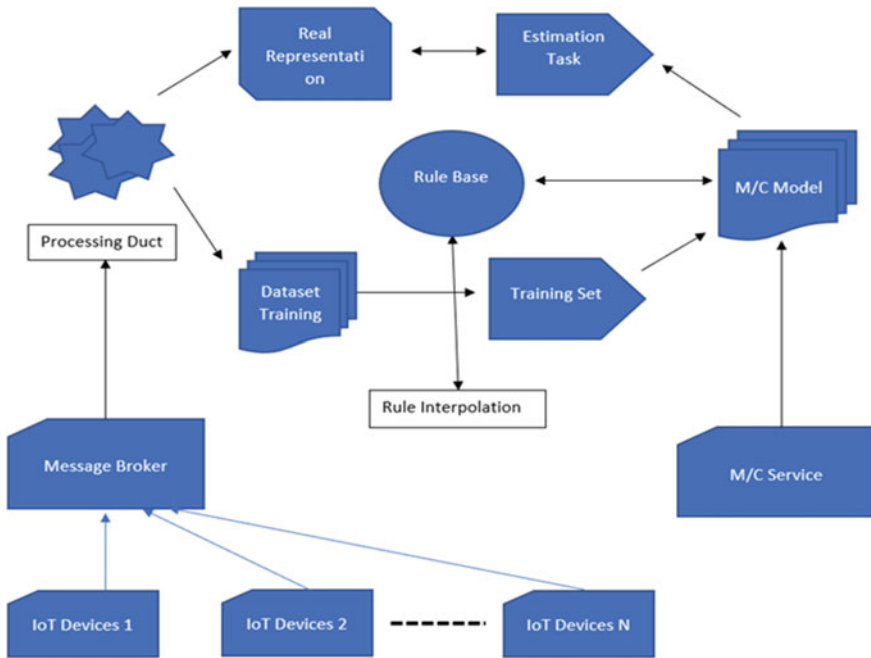


Fig. 2 Modified MQTT broker

will send the topic to the broker and it will be subscriber who receives the message from the broker (Fig. 2).

Publisher (Topic, DATA);

Subscriber (Topic, DATA);

When the incoming packets are added into the broker MQTT, it is segmented into 5 tuples as,

- Source IP
- Destination IP
- Prototype.
- Source Port
- Destination Port

By using the above tuples, the flow can be analysed by adding modified C 4.5 decision tree with modified random forest integration and estimator, which helps to determine the probability of the class of each output variable Y given a set of input features x_1, \dots, x_n .

In this IoT devices, messages are sent through central broker of cloud-based public service through communication protocol of modified MQTT. Here, the cloud-based service framework is used to consume message from multiple devices with reduced cost and data reliability among the sensor data. Message broker subscribes to some stream process and makes them to process actively to represent the real

representation. This machine learning helps the streaming process to perform the analysis real time. The machine learning model helps to train the dataset and task estimation effectively.

3.1 Modified Random Forest Algorithm

Prerequisite: Number of trees to be made in the forest is represented by N, training dataset T and input features F.

Function random_forest(T,E)

R \rightarrow δ

For $i \in 1, \dots, N$ do

T(i) \rightarrow Sample from T

R_i \rightarrow random tree metadata (T(i), E)

R \rightarrow R U {R_i}

end for

return R

end function

function random tree_metadata_learn(T, E)

At each node:

F \rightarrow small mode of E

Split for best feature in E

Return tree after successful learning phase

End Function

Algorithm of detection system for Distributed DoS: (Pseudocode)

```

Input: Information flow in the network
Output: Decision process
START
Intruder -> ZERO
Estimate the arrival time of the publisher on MQTT protocol
Select the constraint based on CONNECT and CONNACK
Determine the connect and acknowledgment ratio
Training the dataset value
Find the estimated values
Check the rule base interpolation
    If Base Rule is Found
        Defuzzification
    Else
        Apply rule interpolation
    For anomaly detection,
    If anomaly -> true
        Decision Process -> Packet Drop
    Else
        Decision Proces -> Packet Accepted
STOP
    
```

4 Results

To provide various QoS parameter like large resource usage, packet loss, packet overhead, throughput and time complexity. Analyse the anomaly detection system with periodic time with respect to the data communication in IoT device network. Comparison table with existing methods [13, 21] (Tables 1 and 2).

Table 1 Comparison of existing method based on malicious node detection

Existing algorithm	Malicious node detection (Time frame)
Secure MQTT [13]	17
MQTT S [21]	14
Classical MQTT [22]	10
Signature-based IDS [23]	6

Table 2 Comparison of existing method based on detection rate (%)

Existing algorithm	Detection rate (%)
Secure MQTT	85
MQTT S	75
Classical MQTT	60
Signature-based IDS	55

5 Conclusion and Future Scope

Improved and secure MQTT strategy to monitor and detect the network activity for heterogenous IoT network is associated with proposed machine learning approach with QoS parameters like large resource usage, packet loss, packet overhead, throughput and time complexity. The detection system based on IDS should be supported with heterogenous features of IoT device network. Provide effective monitoring of network activity with less energy consume and data scalability.

References

1. Atzori L, Iera A, Morabito G (2010) The Internet of Things: a survey. *Comput Netw* 54(15):2787–2805
2. Sethi P, Sarangi SR (2017) Internet of Things: architectures, protocols, and applications. *Can J Electr Comput Eng* 2017(2017):1–25
3. Ammar M, Russello G, Crispo B (2018) Internet of things: a survey on the security of IoT frameworks. *J Inf Secur Appl* 38:8–27
4. Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC (2017) A survey of intrusion RJR. *J Netw Comput Appl* 84:25–37
5. Roesch M (1999) Snort: lightweight intrusion detection for networks. *Lisa* 99(1):229–238
6. Oh D, Kim D, Ro WW (2014) A malicious pattern detection engine for embedded security systems in the Internet of Things. *Sensors* 14(12):24188–24211
7. Cho E, Kim J, Hong C (2009) Attack model and detection scheme for botnet on 6LoWPAN. In: *Management enabling the future internet for changing business and new computing services (Lecture notes in computer science)*, vol 5787. Springer, Berlin, Heidelberg, pp 515–518
8. Stephen R, Arockiam L (2017) Intrusion detection system to detect sinkhole attack on RPL protocol in Internet of Things. *Int J Electr Electron Comput Sci* 4(4):16–20
9. Shamshirband S, Patel A, Anuar NB, Kiah MLM, Abraham A (2014) Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks. *Eng Appl Artif Intell* 32:228–241
10. Arshad J, Abdellatif MM, Khan MM, Azad MA (2018) A novel framework for collaborative intrusion detection for M2M networks. In: *Proceedings of 9th international conference on information and communication systems (ICICS)*
11. Lavrova D, Pechenkin A (2015) Applying correlation and regression analysis to detect security incidents in the internet of things. *Int J Commun Netw Inf Secur* 7(3):131
12. Raza S, Wallgren L, Voigt T (2013) SVELTE: real-time intrusion detection in the Internet of Things. *Ad Hoc Netw* 11(8):2661–2674
13. Wallgren L, Raza S, Voigt T (2013) Routing attacks and countermeasures in the RPL-based internet of things. *Int J Distrib Sens Netw* 9(8):794326

14. Shimeall TJ, Spring JM (2014) Recognition strategies: intrusion detection and prevention. In: Introduction to information security: a strategic-based approach. Elsevier, pp 253–274
15. Yassein MB, Shatnawi MQ, Aljwarneh S, Al-Hatmi R (2017) Internet of Things: survey and open issues of MQTT protocol. In: Proceedings of international conference on engineering & MIS (ICEMIS)
16. Singh M, Rajan MA, Shivraj VL, Balamuralidhar P (2015) Secure MQTT for Internet of Things (IoT). In: Proceedings of fifth international conference on communication systems and network technologies
17. Deshai N, Sekhar BVDS, Reddy PVGD, Chakravarthy VVSSS (2020) Processing real world datasets using big data Hadoop tools. *J Sci Ind Res (JSIR)* 79(7):631–635
18. Balasundaram A, Kothandaraman D, Kumar PS, Ashokkumar S (2020) An approach to secure capacity optimization in cloud computing using cryptographic hash function and data de-duplication. In: 2020 3rd international conference on intelligent sustainable systems (ICISS), pp 1256–1262
19. Harshavardhan A, Ramesh D, Pasha SN, Shwetha S, Mohmmad S, Kothandaraman D (2020) Lifting wheelchair for limbless people. *IOP Conf Ser Mater Sci Eng* 981(2):022036
20. Kumar BV, Korra SN, Swathi N, Kothandaraman D, Yamsani N, Chanti Y (2020) Traffic control system for vehicles on Indian roads using raspberry Pi. *IOP Conf Ser Mater Sci Eng* 981(3):032098
21. Venkataramana S, Sekhar BVDS, Raju VS, Chakravarthy VVSSS, Srinivas G (2020) An experimental analysis of secure-energy trade-off using optimized routing protocol in modern-secure-WSN. *EAI Endorsed Trans Scalable Inf Syst* 7(26)
22. Malina L, Srivastava G, Dzurenda P, Hajny J, Fujdiak R (2019) A secure publish/subscribe protocol for internet of things. In: Proceedings of 14th international conference on availability, reliability and security, pp 1–10
23. Almutairi AH, Abdelmajeed NT (2017) Innovative signature-based intrusion detection system: parallel processing and minimized database. In: Proceedings of international conference on the frontiers and advances in data science (FADS)

Optimal Codebook Construction Method Based on Zadoff-Chu Matrix for Code Division Multiple Access Systems



R. Nirmaladevi and K. Kishan Rao

Abstract Codebooks with low correlation properties have important applications in synchronous code division multiple access systems (CDMA), quantum information theory, and compressed sensing. In order to expand the number of codebooks, the restriction conditions of the transformation matrix are relaxed. Based on the Zadoff-Chu matrix, a new codebook is constructed using difference set, almost difference set, and finite field features, and the obtained codebook is optimal or almost optimal according to Welch bound or Levenstein bound. Through experimental simulation, it is found that the deterministic measurement matrix constructed based on this type of codebook has good performance in compressed sensing.

Keywords Codebook · Difference set · Almost difference set · Welch bound · Levenstein bound

1 Introduction

Codebook is a type of signal set with low correlation, which has important applications in synchronous code division multiple access (CDMA, code division multiple access) communication systems [1], quantum coding theory [2], and compressed sensing [3]. It is one of the important research topics of modern communication theory to construct the optimal codebook whose parameters reach the theoretical limit. Therefore, the research of the codebook construction method has attracted widespread attention. Generally speaking, the codebook C is represented by two

R. Nirmaladevi (✉)

Department of Electronics and Instrumentation Engineering, KITS Warangal, Warangal, Telangana, India

e-mail: nimala123@yahoo.com

Research Scholar, Department of ECE, JNTUH University, Hyderabad, Telangana 500085, India

K. Kishan Rao

Department of Electronics and Communication Engineering, Srinidhi Institute of Science and Technology, Hyderabad, Telangana, India

parameters, namely (N, K) , where N represents the number of codebooks, and K represents the length of the codebook. The character set of the codebook is the set of different complex values used by the coordinates of all codewords in the codebook, and the size of the character set is the number of elements in the character set. In practical applications, a codebook with a smaller character set is of great significance. In addition, the maximum cross-correlation amplitude value of the codebook is represented by $I_{\max}(C)$. In a communication system, it is hoped that the maximum cross-correlation amplitude $I_{\max}(C)$ of the codebook is as small as possible to eliminate interference between signals as much as possible. In the field of compressed sensing, codebooks with low correlation can be used to construct measurement matrices.

According to the theory of compressed sensing, the lower the maximum cross-correlation amplitude values of the codebook, the better the performance of the corresponding measurement matrix restricted isometric property (RIP) [2]. In addition, in the field of quantum information [3], codebooks are also used to construct symmetric informational complete positive operator-valued measure (SIC-POVM) and unbiased orthogonal bases (MUB). The parameters of the codebook are restricted by theoretical limits. When $N \geq K$, the codebook whose maximum cross-correlation amplitude value meets the Welch limit is called the optimal codebook, it is said that the maximum cross-correlation amplitude value meets the Levenstein limit. The codebook is the optimal codebook. In recent years, researchers have proposed many codebook construction methods that approximate the Welch bound or Levenstein bound. Literature [4] first constructed the optimal codebook by using the difference set. Ding et al. [5, 6] further used difference sets and almost difference sets to construct an optimal codebook whose parameters reached the Welch bound. Literature [7–10] uses the cyclotomic method to construct a codebook with excellent parameters. In addition, there are some methods to construct codebooks using bent functions [11], flat functions [12], features and theories on finite fields [13–16], and binary linear codes [17].

In recent years, literature [18] proposed a codebook construction framework based on binary sequences and transformation matrices. The framework includes many existing codebook construction methods, such as the method in literature [4–6]. This type of method has two key factors: (1) the construction of the transformation matrix that satisfies certain conditions; (2) the selection of the binary sequence support set. Most of the existing codebook construction methods are based on existing transformation matrices such as inverse discrete Fourier transform (IDFT) matrix, Hadamard matrix, and the codebook is constructed by selecting different binary sequence support sets. Based on the same idea, literature [19, 20] constructed a new type of optimal codebook by selecting a new type of binary sequence. This paper relaxes the conditional restrictions on the initial transformation matrix in the literature [18], constructs a new type of transformation matrix, and combines some existing special integer sets to construct a codebook whose parameters reach the asymptotic optimality.

2 Conceptual Working Model

A codebook with parameters (N, K) is a set of complex vectors $C = \{C_0, C_1, \dots, C_{N-1}\}$, where each vector, $C_n = (c_{n,0}, c_{n,1}, \dots, c_{n,K-1})$ is a unit complex vector of length K , where $0 \leq n \leq N-1$, $\sum_{k=0}^{K-1} (c_{n,k})^2 = 1$. For any two vectors $C_{n_1}, C_{n_2} \in C$, define the Hermitian inner product as $C_{n_1} (C_{n_2})^H = \sum_{k=0}^{K-1} c_{n_1,k} c_{n_2,k}^*$, where $(\cdot)^H$ represents the vector conjugate transpose. The maximum cross-correlation magnitude value in the vector set C is defined as

$$I_{\max}(C) = \max_{0 \leq n_1 \neq n_2 \leq N-1} |C_{n_1} (C_{n_2})^H| \quad (1)$$

For the maximum cross-correlation amplitude value of the codebook, the following limits are established. For a codebook C [4] with parameters (N, K) , where $N \geq K$, then we have

$$I_{\max}(C) \geq \sqrt{\frac{N-K}{(N-1)K}} \quad (2)$$

The condition that the equal sign of formula (2) holds is if and only if for any $0 \leq n_1 \neq n_2 \leq N-1$, there is

$$|C_{n_1} (C_{n_2})^H| = \sqrt{\frac{N-K}{(N-1)K}} \quad (3)$$

When formula (3) is established, the maximum cross-correlation amplitude value of the codebook reaches the Welch boundary, which is called maximum-Welch bound-equality (MWBE) codebook; when $N > K^2$, there is no (N, K) that reaches the Welch boundary. Codebook, at this time the Levenstein bound is tighter.

For real codebooks [11] with arbitrary parameters (N, K) , if $N > \frac{K(K+1)}{2}$, then

$$I_{\max}(C) \geq \sqrt{\frac{3N - K^2 - 2K}{(N-K)(K+2)}} \quad (4)$$

For a complex codebook with any parameter (N, K) , if $N > K^2$, then there is

$$I_{\max}(C) \geq \sqrt{\frac{2N - K^2 - K}{(N-K)(K+2)}} \quad (5)$$

Generally, the codebook that reaches the Welch bound or Levenstein bound is called the optimal codebook, which has important application value for the research on the construction method of the optimal codebook.

Let p be a prime number, F_p denote a finite field containing p elements, $F_p^* = F_p \setminus \{0\}$. Let $Z_N = \{0, 1, 2, \dots, N - 1\}$ denote a ring of integers modulo N . Suppose $q = p^n$ is a prime number power, p is a prime number, let α denote the generator of the cyclic group $F_{q^s}^*$, and the multiplication feature on the finite field F_{q^s} is defined as

$$\chi_a(\alpha^i) = \omega_{q^s-1}^{ai}, \quad a \in F_{q^s}, \quad 0 \leq i \leq q^s - 2 \tag{6}$$

where $\omega_{q^s-1} = e^{\frac{2\pi\sqrt{-1}}{q^s-1}}$. when $a = 0$, call χ_a as a trivial multiplication feature, otherwise call χ_a as a non-trivial multiplication feature. Define $\chi(0) = 0$, for the multiplication feature, satisfy $\chi(xy) = \chi(x)\chi(y)$, $x, y \in F_{q^s}$. Suppose the set $D = \{d_0, d_1, \dots, d_{K-1}\}$ denotes a subset of the finite field F_p , and the difference function of the set D is defined as $f_D(\tau) = |(\tau + D) \cap D|$, $\tau \in F_p$. If it is satisfied that when τ is taken over the non-zero elements on F_p , the difference function $f_D(\tau)$ takes the value of λ and appears $p - 1$ times, then the set D is said to be a difference set on the finite field F_p , and the parameters are expressed as

$$(p, K, \lambda) - \text{DS} \tag{7}$$

Obviously, for the difference set $(p, K, \lambda) - \text{DS}$, $K(K - 1)(p - 1)\lambda$ holds. Suppose the set $D = \{d_0, d_1, d_2, \dots, d_{k-1}\}$ denotes a subset of the finite field F_p , and the difference function of the set D is defined as $f_D(\tau) = |(\tau + D) \cap D|$, $\tau \in F_p$. If it is satisfied that when τ is taken over the nonzero elements on F_p , the difference function $f_D(\tau)$ takes the value of λ to appear t times, and the value of $\lambda + 1$ to appear $p - 1 - t$ times, then the set D is said to be a finite field on F_p . An almost difference set of the parameter is expressed as $(p, K, \lambda, t) - \text{ADS}$. Let $D = \{d_0, d_1, d_2, \dots, d_{K-1}\}$ which represents a set of K different integers on the integer ring $d_k \in Z_J$, $0 \leq k \leq K - 1$. The characteristic sequence of set D is defined as a binary sequence $= (a_0, a_1, \dots, a_{J-1})$, where.

$$a_t = \begin{cases} \exp\left(-\frac{i\pi\gamma k(k+2g)}{N}\right), & N \text{ is even} \\ \exp\left(-\frac{i\pi\gamma k(k+1+2g)}{N}\right), & N \text{ is odd} \end{cases} \quad \text{where } k = 0, 1, \dots, N - 1, g \text{ is an integer} \tag{8}$$

3 Conceptual Working Model

Literature [18] proposed a kind of codebook construction framework based on binary sequence, and its construction process is as follows.

Step 1: Define a transformation matrix, $\Phi = [\phi_{i,l}]_{J \times N}$, let $\phi_{i,l}$ denote any element in the matrix, $0 \leq i \leq J - 1, 0 \leq l \leq N - 1$. The matrix $\Phi = [\phi_{i,l}]_{J \times N}$ satisfies the following properties.

- Each matrix element has unit amplitude, that is, $|\phi_{i,l}| = 1$.
- Any two different column vectors satisfy $\phi_{i,l_1}^* \phi_{i,l_2} = \phi_{i,l}, 0 \leq l_1 \neq l_2, l \leq N - 1, 0 \leq i \leq J - 1$.
- The first column of matrix Φ is a vector of all ones, i.e., $\phi_{i,0} = 1, 0 \leq i \leq J - 1$.
- For any $0 < l \leq N - 1$, there are $\sum_{i=0}^{J-1} \phi_{i,l} = 0$.

The transformation matrix that satisfies the above properties is known to be $N \times N$ Hadamard matrix and IDFT matrix.

Step 2: Take the binary sequence $a = (a_0, a_1, \dots, a_{J-1})$, the Hamming weight of the sequence $wt(a) = K$, and set the set $D = \{d_0, d_1, d_2, \dots, d_{K-1}\}$ to be the sequence a Support set. Construct codebook $C_\Phi(a) = \{C_0, C_1, \dots, C_{N-1}\}$ is

$$C_l = \frac{1}{\sqrt{K}} (\phi_{d_0,l}, \phi_{d_1,l}, \dots, \phi_{d_{K-1},l}), 0 \leq l \leq N - 1 \quad (9)$$

where C_l is a row vector in the constructed codebook, set D is the row index set of the transformation matrix Φ , that is, the element, $\phi_{d_k,l} (0 \leq k \leq K - 1)$ is the d_k row and l -th row in the matrix column elements, then is the obtained (N, K) codebook, and its maximum cross-correlation amplitude $I_{\max}(C_\Phi(a))$ can be calculated from the support set of the transformation matrix and the binary sequence.

The framework constructed in [18] includes some existing codebook construction methods as special cases. For example, when an IDFT matrix of order $N \times N$ is selected as the transformation matrix Φ , if the support set corresponding to the selected binary sequence is the difference set, the codebook $C_\Phi(a)$ obtained is the result of the document [4]. If the binary or complex Hadamard matrix is used as the matrix Φ , when the selected binary sequence corresponding to the support set is an almost difference set, the codebook $C_\Phi(a)$ obtained is the result of literature [5, 6]. The structural framework has two key factors: (1) selection of transformation matrix Φ ; (2) selection of support set of binary sequence a . Based on this construction framework, literature [19] constructed a codebook with almost optimal parameters by selecting different binary sequences. At the same time, the literature [19] also pointed out that a new codebook can be constructed by constructing a new transformation matrix, but it does not give a new transformation matrix construction method. Literature [20] also uses Hadamard matrix as the transformation matrix and constructs a class of optimal codebooks by designing a new class of binary sequences. From another perspective, this article constructs a new codebook by designing a new transformation matrix.

4 Optimal Codebook Construction

The new construction method proposed in this paper is introduced as follows.

Step 1: According to definition 5, let $g = 0$, $\gamma = 1$, N be even numbers, and get the first row of the Zadoff-Chu matrix. Let $\phi_k = e^{\frac{-i\pi k^2}{N}}$, $k = 0, 1, \dots, N - 1$, from this define the Zadoff-Chu matrix $\Phi = [\phi_{s,t}]_{N \times N}$ as

$$K\phi_{s,t} = e^{\frac{-i\pi\sqrt{-1}(s-t)^2}{N}} \quad (10)$$

where $0 \leq s, t \leq N - 1$. In [21], let the N of matrix Φ be an even number to construct the measurement matrix, and this paper takes the case of N as an odd number to construct the codebook.

Step 2: Suppose $D = \{d_0, d_1, d_2, \dots, d_{K-1}\}$ which represents a set of K different integers on the integer ring $d_k \in \mathbb{Z}_N$, $0 \leq k \leq K - 1$. Construct the codebook

$$C_\Phi = \{C_0, C_1, \dots, C_{N-1}\} \quad (11)$$

Then C_Φ is the obtained (N, K) codebook. Let C_Φ be the (N, K) codebook obtained by the new construction method in this paper, then the maximum correlation amplitude value is

$$I_{\max}(C_\Phi) = \frac{1}{K \left| \sum_{d_k \in D} w_N^{\Delta d_k} \right|} \quad (12)$$

where $0 < |\Delta| \leq N - 1$ is a nonzero real number.

Suppose, $C_l, C_t \in C_\Phi$, $0 \leq t \neq l \leq N - 1$, then we have

$$\begin{aligned} |C_t(C_l)^H| &= \left| \frac{1}{K} \sum_{k=0}^{K-1} \phi_{d_k,t} (\phi_{d_k,l})^* \right| \\ &= \frac{1}{K} \left| \sum_{d_k \in D} e^{\frac{-i\pi\sqrt{-1}(t-d_k)^2}{N}} e^{\frac{-i\pi\sqrt{-1}(l-d_k)^2}{N}} \right| \\ &= \frac{1}{K} \left| e^{\frac{\pi\sqrt{-1}(t^2-l^2)}{N}} \sum_{d_k \in D} e^{\frac{2i\pi\sqrt{-1}(l-t)d_k}{N}} \right| \\ &= \frac{1}{K} \left| \sum_{d_k \in D} w_N^{(l-t)d_k} \right| \end{aligned} \quad (13)$$

where $w_N = e^{\frac{2\pi\sqrt{-1}}{N}}$. Let $\Delta = l - t$, so $|C_t(C_l)^H| = 1/K \left| \sum_{d_k \in D} w_N^{\Delta d_k} \right|$, from $0 \leq t \neq l \leq N - 1$ we know that $0 < |\Delta| \leq N - 1$, proposed 1 holds.

4.1 Optimal Codebook Based on Difference Set

Let the set $D = \{d_0, d_1, \dots, d_{K-1}\}$ [5] represents a difference (p, K, λ) on finite field F_p - DS, then for any $\gamma \neq 0 \pmod p$ there is

$$\left| \sum_{k=0}^{K-1} w_p^{\gamma d_k} \right| = \sqrt{\frac{K(p-K)}{p-1}} \tag{14}$$

where $w_p = e^{\frac{2\pi\sqrt{-1}}{p}}$.

Accordingly the following conclusion can be reached. Let $N = p$ prime, and if the set $D = \{d_0, d_1, d_2, \dots, d_{K-1}\}$ is a difference set $(p, K, \lambda) - DS$ on finite F_p , then the code book argument defined in Eq. (9) is (p, K) , the character set size of the code book is $2p$, and the maximum correlation amplitude value is $I_{\max}(C_\Phi) = \sqrt{\frac{p-K}{(p-1)K}}$, and the code book reaches the Welch boundary.

According to lemma1, the maximum relevant amplitude value of the codebook is equal to the Welch bounds, which is an optimal class of codebooks. Let $p = 7$ take the set $D = \{1, 2, 4\}$, which shows that it is a difference set $(7, 3, 1) - DS$, and the code $(7, 3)$ is obtained

$$\begin{aligned} C_0 &= \frac{1}{\sqrt{3}}(\zeta_7^1, \zeta_7^4, \zeta_7^2), C_1 = \frac{1}{\sqrt{3}}(\zeta_7^0, \zeta_7^1, \zeta_7^9), \\ C_2 &= \frac{1}{\sqrt{3}}(\zeta_7^1, \zeta_7^0, \zeta_7^4), C_3 = \frac{1}{\sqrt{3}}(\zeta_7^4, \zeta_7^1, \zeta_7^1) \\ C_4 &= \frac{1}{\sqrt{3}}(\zeta_7^9, \zeta_7^4, \zeta_7^0), C_5 = \frac{1}{\sqrt{3}}(\zeta_7^2, \zeta_7^9, \zeta_7^1), C_6 = \frac{1}{\sqrt{3}}(\zeta_7^{11}, \zeta_7^2, \zeta_7^4) \end{aligned} \tag{15}$$

where $\zeta_7 = e^{-\frac{\pi\sqrt{-1}}{7}}$. The maximum correlation amplitude value for this codebook is 0.4714.

The resulting codebook of the proposed 2 has the same parameters and the same maximum correlation amplitude as the document [4, 18], but is not the same type of codebook. Due to the different choices of transformation matrices, the elements inside the Type 2 codebook are also different. The transformation matrix selected for the codebook [4, 18] of the document [4, 18] is the IDFT matrix with a smaller character set; the transformation matrix of the codebook constructed by the proposed 2 is the Zadoff-Chu matrix, which has fewer restrictions and is more flexible in construction.

For example, the same difference set $D = \{1, 2, 4\}$ is chosen, and the code book obtained by the document [4, 18] is

$$\begin{aligned}
 C_0 &= \frac{1}{\sqrt{3}}(w_7^0, w_7^0, w_7^0), C_1 = \frac{1}{\sqrt{3}}(w_7^1, w_7^2, w_7^4), \\
 C_2 &= \frac{1}{\sqrt{3}}(w_7^2, w_7^4, w_7^1), C_3 = \frac{1}{\sqrt{3}}(w_7^3, w_7^6, w_7^5), \\
 C_4 &= \frac{1}{\sqrt{3}}(w_7^4, w_7^1, w_7^2), C_5 = \frac{1}{\sqrt{3}}(w_7^5, w_7^3, w_7^6), C_6 = \frac{1}{\sqrt{3}}(w_7^6, w_7^5, w_7^3)
 \end{aligned}
 \tag{16}$$

where $w_7 = e^{-\frac{\pi\sqrt{-1}}{7}}$.

4.2 Optimal Codebook Based on Almost Difference Set

Let $p = ef + 1$ be a prime number, where e and f are positive integers. Define the set $D_i^{(e,p)} = \{\alpha^j | \alpha \in F_p^*, j = i \text{ mod } ee\}$ is the e -order cyclotomic class on the finite field F_p [5]. Let $p \equiv 1 \pmod{4}$, then the second-order cyclotomic class $D_0^{(2,p)}$ is the almost difference set on the finite field F_p , and the parameters are, $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{2}) - ADS$. For this almost difference set, $\Delta \neq 0$, there is

$$\sum_{d_k \in D_0^{(2,p)}} w_p^{\Delta d_k} = \frac{-1 \pm \sqrt{p}}{2}
 \tag{17}$$

Let N_p be a prime number, if the set $D = \{d_0, d_1, d_2, \dots, d_{K-1}\}$ is the almost difference set on the finite field F_p , $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{2}) - ADS$, that is $D = D_0^{(2,p)}$, then the codebook parameter defined by Eq. (9) is, $(p, \frac{p-1}{2})$, the character set size of the codebook is $2p$, The maximum correlation amplitude value is $I_{\max}(C_\Phi) = \frac{1+\sqrt{p}}{p-1}$. The codebook gradually reaches the Welch world. According to the construction process, we can know the number of vectors N_p and the length of the vectors $K = \frac{p-1}{2}$, and the cross-correlation magnitude is calculated as follows. From Lemma 4, we know that for the almost difference set $D = D_0^{(2,p)}$, there are $\left| \sum_{d_k \in D_0^{(2,p)}} w_p^{\Delta d_k} \right| \leq \frac{1+\sqrt{p}}{2}$. Again by, the maximum correlation amplitude of the codebook is $I_{\max}(C_\Phi) = \frac{1+\sqrt{p}}{2} \frac{2}{p-1} = \frac{1+\sqrt{p}}{p-1}$. Accordingly, for $(p, \frac{p-1}{2})$ codebook, the Welch bound of the correlation amplitude value is $\text{Welch } I_{\text{welch}}(C_\Phi) = \frac{\sqrt{p+1}}{p-1}$. Then there is

$$\lim_{p \rightarrow \infty} \left\{ \frac{I_{\max}(C_{\Phi})}{I_{\text{welch}}(C_{\Phi})} \right\} = \lim_{p \rightarrow \infty} \left\{ \frac{1 + \frac{1}{\sqrt{p}}}{\sqrt{1 + \frac{1}{p}}} \right\} = 1 \quad (18)$$

It is seen that when p increases, the codebook gradually reaches the Welch bound.

4.3 Optimal Codebook Based on Feature Sum

Let ξ_K denotes the set formed by the orthonormal basis of the K -dimensional Hilbert space, that is, the set consisting of the following K vectors of length $K(1)$ i.e., $1 \leq i \leq K$. Let $q = p^n$ be a power of a prime number, where p is a prime number. Let $a \in F_q^*$, define the $T_a = \left\{ x \in F_q^* \mid \text{Tr}_{F_q^s/F_q}(x) = a \right\}$, with $|T_a| = q^{s-1}$. The Eisenstein sum on the finite field F_{q^s} is defined as

$$E_1(\chi) = \sum_{x \in T_1} \chi(x) \quad (19)$$

Define $E_a(\chi) = \sum_{x \in T_a} \chi(x)$, obviously for $a \in F_q^*$ there is $E_a(\chi) = \chi(a)E_1(\chi)$.

$$|E_a(\chi)| \in \left\{ q^{\frac{s-1}{2}}, q^{\frac{s-2}{2}} \right\} \quad (20)$$

Let C_{Φ} be defined by the expression (9) Codebook, then $C_{\Phi} \cup \xi$ is the $(q^2 + q - 1, q)$ codebook, the character set size of the codebook is $2p + 1$, and the maximum cross-correlation amplitude is $I_{\max}(C_{\Phi} \cup \xi_k) = \frac{1}{\sqrt{q}}$. Proof From the above construction process, we know the vector length a $K = |T_a| = q^{s-1} = q$, and the number of vectors is $N = q^2 + q - 1$.

5 Comparative Analysis of Optimal Codebook Construction Methods

It can be seen that according to the codebook construction framework proposed in [18], codebooks with different parameters can be constructed by selecting different transformation matrices and sets. The existing methods are based on IDFT matrix or Hadamard matrix, using different sets to construct the codebook. This paper proposes a new type of transformation matrix, which uses the existing difference set, almost difference set, and a set defined by Eisenstein on the finite field to construct a codebook with optimal parameters and asymptotically optimal parameters. The same parameters and maximum correlation magnitude as the optimal codebooks in the

existing literature [4, 18] and literature [5], so they can provide more choices for communication systems or information processing.

Proposed constructs a new type of codebook, which is asymptotically optimal according to the Levenstein bound, and has a smaller maximum cross-correlation magnitude compared to the asymptotically optimal codebook according to the Welch bound. Although the new transformation matrix relaxes the restrictions and makes the character set larger, when constructing the codebook with the same parameters, the transformation matrix has more flexibility in the selection. The codebook constructed in this paper is a better choice in applications that do not require character sets, such as constructing the deterministic measurement matrix of compressed sensing. Example 2 Let $p = 67$, the difference set, construct a codebook with a parameter of $(67, 33)$, and the maximum correlation amplitude reaches the Welch bound. Let $p = 61$, the almost difference set, construct a codebook with a parameter of $(61, 30)$ and the maximum correlation amplitude asymptotically reaches the Welch bound. Through the method of literature [3], the constructed codebook is applied to the compressed sensing to construct the deterministic measurement matrix. The size of the measurement matrix obtained accordingly is set to 33×67 , and the size of the measurement matrix obtained accordingly is set to 30×61 . The maximum cross-correlation amplitude reaches and asymptotically reaches the Welch bound, respectively. The codebook constructed has the same parameters as the codebook constructed based on the IDFT matrix and difference set in literature [4, 18], so the codebook in literature [4, 18] is also constructed as a deterministic measure matrix. Then select the same size random discrete Fourier transform (DFT) matrix and random complex Gaussian matrix as random measurement matrices for signal recovery and comparative analysis, and the obtained signal reconstruction probability versus sparsity curve is shown in Fig. 1.

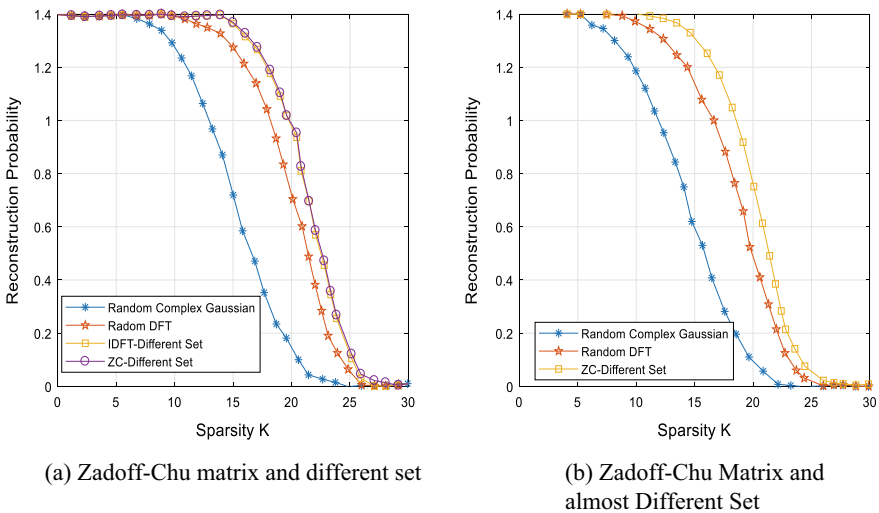


Fig. 1 Variation curve of sparsity with reconstruction probability

It can be seen from Fig. 1a that the probability of reconstructing the signal is significantly higher than that of random DFT matrix and random complex Gaussian matrix when the deterministic measurement matrix constructed by the codebook in this paper has the same sparsity. The deterministic measurement matrix constructed using the same parameters as the measurement matrix constructed using the literature [4, 18], and the probability of reconstructing the signal is even slightly higher than the method in the literature [4, 18]. In the same way, the deterministic measurement matrix constructed using the codebook in Proposed 3 of this paper has a significantly higher probability of reconstructing the signal than the random measurement matrix.

6 Conclusion

Based on the codebook construction idea of literature [18], this paper relaxes the restriction conditions of the transformation matrix and proposes a new type of Zadoff-Chu matrix, and uses the features of difference set, almost difference set and finite field to construct 3 types Codebook, the parameters are (p, K) , $(p, \frac{p-1}{2})$ and $(q^2 + q - 1, q)$. The codebook constructed in this paper has the same parameters and maximum cross-correlation amplitude value as the existing codebook and can reach the optimal or progressively optimal. The method in this paper can provide a large number of available codebooks for synchronous CDMA communication systems, and the codebook obtained in this paper can be applied to the construction of the deterministic measurement matrix in the compressed sensing field through the method of literature [3], and the obtained deterministic measurement matrix is important that the probability of constructing the signal is obviously better than the random measurement matrix.

References

1. Ding CS, Golin M, Klove T (2003) Meeting the Welch and Karystinos Pados bounds on DS-CDMA binary signature sets. *Des Codes Crypt* 30(1):73–84
2. Feng KQ, Jin LF (2017) Several mathematical problems in quantum information theory. *Scientia Sinica (Mathematics)* 47(11):1387–1408
3. Li SX, Ge G (2014) Deterministic sensing matrices arising from near orthogonal systems. *IEEE Trans Inf Theor* 64(4):2291–2302
4. Xia PF, Zhou SL, Giannakis GB (2005) Achieving the welch bound with difference sets. *IEEE Trans Inf Theor* 51(5):1900–1907
5. Ding CS (2006) Complex codebooks from combinatorial designs. *IEEE Trans Inf Theor* 52(9):4229–4235
6. Ding CS, Feng T (2008) Codebooks from almost difference sets. *Des Codes Crypt* 46:113–126
7. Zhang AX, Feng KQ (2015) Construction of a class of codebooks nearly meeting the welch bound. *Scientia Sinica (Informations)* 45(12):1632–1639
8. Li CJ, Yue Q, Huang YW (2015) Two families of nearly optimal codebooks. *Des Codes Crypt* 75(1):43–57

9. Zhang AX, Feng KQ (2012) Construction of cyclotomic codebooks nearly meeting the Welch bound. *Des Codes Crypt* 63(2):209–224
10. Zhang AX, He CY, Ji Z (2018) Constructions of some classes of codebooks nearly meeting the Welch bound. *Pure Appl Math* 34(3):323–330
11. Venkataramana S, Sekhar BVDS, Deshai N, Chakravarthy VVSSS, Rao SK (2019, May) Efficient time reducing and energy saving routing algorithm for wireless sensor network. *J Phys: Conf Ser* 1228(1):012002 IOP Publishing
12. Qu LJ (2016) A new approach to constructing quadratic pseudo-planar functions over \mathbb{F}_2^n . *IEEE Trans Inf Theor* 62(11):6644–6658
13. Heng ZL, Ding CS, Yue Q (2017) New constructions of asymptotically optimal codebooks with multiplicative characters. *IEEE Trans Inf Theor* 63(10):6179–6187
14. Heng ZL (2018) Nearly optimal codebooks based on generalized Jacobi sums. *Discrete Appl Math* 250:227–240
15. Luo GJ, Cao XW (2018) Two constructions of asymptotically optimal codebooks via the hyper Eisenstein sum. *IEEE Trans Inf Theor* 64(10):6498–6505
16. Luo GJ, Cao XW (2018) Two constructions of asymptotically optimal codebooks. *Crypt Commun* 11(4):825–838
17. Xiang C, Ding CS, Mesnager S (2015) Optimal codebooks from binary codes meeting the Levenshtein bound. *IEEE Trans Inf Theor* 61(12):6526–6535
18. Yu NY (2012) A construction of codebooks associated with binary sequences. *IEEE Trans Inf Theor* 58(8):5522–5533
19. Cao XW, Chou WS, Zhang XY (2017) More constructions of near optimal codebooks associated with binary sequences. *Adv Math Commun* 11(1):187–202
20. Hong S, Park H, No J (2014) Near optimal partial Hadamard codebook construction using binary sequences obtained from quadratic residue mapping. *IEEE Trans Inf Theor* 60(6):3698–3705
21. Wang X, Zhang J, Ge G (2016) Deterministic convolutional compressed sensing matrices. *Finite Fields Appl* 42:102–117

Binary Optimal Low-Correlation Region Sequence Set Construction Method



R. Nirmaladevi and K. Kishan Rao

Abstract Pseudo-random sequences are often used in several multiple access systems to get rid of the possible noise which is very low in bandwidth. It is possible to generate a base sequence with a period variation in order to meet certain conditions. This is demonstrated in this paper using the interleaving method. Further, a class of parameters are obtained for analysis using these base sequence with the objective of best low-correlation zone sequence set. This type of low correlation zone sequence set has a larger number of sequences. It can support more users when applied to a quasi-synchronous CDMA system.

Keywords Pseudo-random sequence · Low correlation zone sequence · Quasi-synchronous CDMA system

1 Introduction

In recent years, the quasi-synchronous CDMA communication system has attracted widespread attention [1, 2]. Different from the traditional CDMA system, the quasi-synchronous CDMA system allows a few chip delays while maintaining the same performance, which solves the most difficult synchronization problem of the traditional CDMA system. It can effectively reduce or even eliminate multiple access interference (MAI) and multipath interference (MPI). This requires that the spreading

R. Nirmaladevi (✉)
Department of Electronics and Instrumentation Engineering, KITS Warangal, Warangal,
Telangana, India
e-mail: nimala123@yahoo.com

Department of ECE, JNTUH University, Hyderabad, Telangana 500085, India

K. Kishan Rao
Department of Electronics and Communication Engineering, Srinidhi Institute of Science and
Technology, Hyderabad, Telangana, India

sequence used in this system not only has a very low autocorrelation value and cross-correlation value when the relative displacement is zero, but also requires autocorrelation and cross-correlation values when there are a few chip relative displacements. It is also very low. This new type of spreading sequence is called a low correlation zone sequence (LCZ). The performance of the low correlation zone sequence set directly affects the performance of the quasi-synchronous CDMA system. Therefore, constructing a low correlation zone sequence integration with a large correlation zone length and a larger number of sequences is a hot issue in the field of spread spectrum sequence design. In recent years, many methods for constructing LCZ sequence sets have been proposed [2–13]. Literature [2] constructed a binary LCZ sequence set based on the GMW sequence, and literature [3] extended the literature [2] construction method and proposed a method for constructing a P-element LCZ sequence set. Literature [4] uses different initial sequences to construct binary and P-element LCZ sequence sets. Literature [5] uses the idea of subdomain decomposition to propose a more systematic LCZ sequence set construction method, including the above several LCZ sequence set construction methods as special cases. Literature [6] proposed a class of LCZ sequence set construction method based on the idea of interleaving. It can be seen from this interleaving method that a type of LCZ sequence set can be obtained as long as the base sequence set that satisfies the condition is constructed. In addition, there are some studies on quaternary LCZ sequence sets [7, 8]. Literature [7] proposed a quaternary LCZ sequence set construction method, which can flexibly set the parameters of the sequence set and use the best binary LCZ sequence set. The best quaternary LCZ sequence set whose sequence number reaches the theoretical limit is constructed. Literature [8] is based on Gray mapping, using binary sequences with ideal autocorrelation or binary low-correlation region sequence sets to construct a quaternary low-correlation region sequence set with the number of sequences close to the theoretical limit. This type of LCZ sequence set can also flexibly set parameters such as the length of the correlation zone and the number of sequences. In this paper, a new type of binary LCZ sequence set is constructed by using binary pseudo-random sequence.

The parameters of the sequence set have reached the boundary [9], which is the best type of binary LCZ sequence set. Compared with the previous method, the initial sequence selection of this method is more flexible, and the obtained sequence set contains more sequences, so it can support more users when applied to the quasi-synchronous CDMA system.

2 Basic Model

Suppose U is a binary sequence set, the number of sequences is M , and the sequence period is N , expressed as $U = \{u_0, u_1, \dots, u_{M-1}\}$, where $u_i = (u_{i,0}, u_{i,1}, \dots, u_{i,N-1})$.

Definition 1 Suppose $u_i, u_j \in U$ and u_i , the periodic cross-j correlation function of sequence u_j is defined as follows:

$$R_{u_i, u_j}(t) = \sum_{t=0}^{N-1} (-1)^{u_{i,t} + u_{j,t+t}} \tag{1}$$

where $0 \leq t < N$, addition is modulo 2 operation, and subscript modulo N operation. $R_{u_i, u_j}(0)$ is called the same cross-correlation function. When $i = j$, call the autocorrelation function of sequence u_i , which can be represented by $R_{u_i}(t)$, and $R_{u_i}(0)$ is called the in-phase autocorrelation function.

Definition 2 Let $u_i, u_j \in U$, when $|t| < T$ with $i \neq j$ or $0 < |t| < T$ and $i = j$, if the sequence correlation function satisfies:

$$|R_{u_i, u_j}(t)| \leq d \tag{2}$$

where d is a small positive number compared with the sequence period T , the sequence set U is called a low correlation zone (LCZ) sequence set, expressed as $LCZ(N, M, T, d)$.

Definition 3 Let $a = (a_0, a_1, \dots, a_{N-1})$ be a binary sequence with a period of N , $a_l \in \{0, 1\}$. If $\sum_{l=0}^{N-1} (-1)^{a_l} = -1$ is established means that the binary sequence a is balanced. If the sequence autocorrelation function satisfies $R_a(t) = -1$ when $t \neq 0 \pmod{N}$, then the sequence a is called an ideal autocorrelation binary sequence. Pseudo-random binary sequences such as m sequence, GMW sequence, cascaded GMW sequence, etc. are ideal autocorrelation binary sequences with balance.

Definition 4 Let $a = (a_0, a_1, \dots, a_{N-1})$ and $b = (b_0, b_1, \dots, b_{N-1})$ be a sequence with two periods of N , if for $0 \leq i \leq N - 1, 0 \leq t \leq N - 1$ has $a_i = b_{i+t}$, it is said that the sequences a and b are shifted equivalent, otherwise it is called shift inequality.

Definition 5 Let $f(x)$ denote a function that maps a finite field F_{2^n} to F_{2^m} , where $m|n$. If for any $r \in F_{2^m}, x \in F_{2^n}$, there are $f(rx) = r^d f(x)$, then it is called a d-form function from F_{2^n} to F_{2^m} .

Lemma 1 [5] Let $h(x)$ be the d-2 form function from F_{2^n} to F_{2^m} in the finite field. If the function $h(x)$ has differential balance, then $h(x)$ has two-state balance [10].

Lemma 2 [10] Let a be an m sequence with a length of $2^m - 1$, and L represents the linear complexity of sequence a . In a cycle of sequence a , the maximum length of a run of 0 is $L - 1$, and the maximum length of a run of 1 is L .

Based on the idea of interleaving, literature [6] proposed a method to construct LCZ sequence set using d-form function. As long as the sequence set meeting the

conditions is constructed as the base sequence, the LCZ sequence set can be obtained by using the interleaving method. In this way, the structure of the low correlation zone sequence set is transformed into the structure of the base sequence set. The following only introduces the main conclusions used in this article.

Lemma 3 [6] *Let S denote a sequence set, the sequence length is $2^m - 1$, if the sequence in the sequence set satisfies the following three conditions.*

1. *All sequences are balanced.*
2. *The mutual correlation value of any two different sequences is -1 .*
3. *All sequences are not equivalent to pairwise shifts.*

Then, using the sequence set S as the base sequence set, a sequence set of n low correlation zone can be obtained, and the parameter is $LCZ(2^n - 1, |S|, \frac{2^n - 1}{2^m - 1}, 1)$ represents the number of sequences in the sequence set S , $m|n$.

It can be seen from Lemma 3 that the construction of the LCZ sequence set is transformed into the construction of the sequence set S that satisfies the conditions. The next section proposes a construction method that uses the m sequence to construct the base sequence set S .

3 Best Binary LCZ Sequence Set Construction Method

This section constructs a new type of LCZ sequence set. Let m and n be positive integers, $(m + 1)n$, and use m sequences with a length of $2^m - 1$ to construct a low correlation zone sequence set.

Let a be an m sequence of length N , and the linear complexity is $L < 2^{m-1}$, $N = 2^m - 1$. Let $(m + 1)n, M = 2^m - 1$.

The base sequence set S that satisfies the conditions of Lemma 3 is constructed in two steps as follows.

Construct shift sequence set $e_j = (e_{j,0}, e_{j,1}), 0 \leq j \leq M - 1$.

$$e_j = (e_{j,0}, e_{j,1}) = (j, N - 1 - j) \tag{3}$$

Use the shift equivalent sequence construction of sequence a to obtain a sequence set $S = \{S_i, 0 \leq i \leq 2M\}$, $S_i = (s_{i,0}, s_{i,1}, \dots, s_{i,2^{m+1}-2})$, the specific process is as follows.

When $0 \leq i \leq M - 1$,

$$s_{i,t} = \begin{cases} a_{t_1+e_{i,0}}, & t = 2t_1 \\ a_{t_1+e_{i,1}}, & t = 2t_1 + 1 \\ 0, & t = 2^{m+1} - 2 \end{cases} \tag{4}$$

where $0 \leq t_1 \leq 2^m - 2$.

When $M \leq i \leq 2M - 1$,

$$S_{i,t} = \begin{cases} a_{t_1+e_{t \bmod M,0}}, & t = 2t_1 \\ a_{t_1+e_{t \bmod M,1}} + 1, & t = 2t_1 + 1 \\ 1, & t = 2^{m+1} - 2 \end{cases} \quad (5)$$

where $0 \leq t \leq 2^m - 2$, and addition is a modulo-2 operation.

When $i = 2M$,

$$S_{M,t} = \begin{cases} 0, & t = 2t_1 \\ 1, & t = 2t_1 + 1 \\ 1, & t = 2^{m+1} - 2 \end{cases} \quad (6)$$

In, $0 \leq t_1 \leq 2^m - 2$.

The sequence set $S = \{S_i, 0 \leq i \leq 2M\}$ obtained by the above method satisfies the three conditions of Lemma 3. To prove that theorem 1 is true, it is only necessary to verify that the sequence set S satisfies the three conditions of Lemma 3.

It is easy to conclude from the balance and construction process of the m sequence that all the sequences in the sequence set S are balanced, and condition 1 is satisfied.

Let S_i and S_j be any two different sequences in the sequence set S . Calculate the same cross-correlation function in the following situations. When $0 \leq i \neq j \leq M-1$ or $M \leq i \neq j \leq 2M-1$,

$$\begin{aligned} R_{S_i, S_j}(0) &= 1 + \sum_{t_1=0}^{2^m-2} (-1)^{a_{t_1+e_{j \bmod M,0}} + a_{t_1+e_{j \bmod M,0}}} + \sum_{t_1=0}^{2^m-2} (-1)^{a_{t_1+e_{j \bmod M,1}} + a_{t_1+e_{j \bmod M,1}}} \\ &= 1 + R_a(e_{j \bmod M,0} - e_{i \bmod M,0}) + R_a(e_{j \bmod M,1} - e_{i \bmod M,1}) \\ &= 1 + (-1) + (-1) \\ &= -1 \end{aligned} \quad (7)$$

When $0 \leq i \leq M-1, M \leq j \leq 2M-1$,

$$\begin{aligned} R_{S_i, S_j}(0) &= -1 + \sum_{t_1=0}^{2^m-2} (-1)^{a_{t_1+e_{i,0}} + a_{t_1+e_{j \bmod M,0}}} - \sum_{t_1=0}^{2^m-2} (-1)^{a_{t_1+e_{i,1}} + a_{t_1+e_{j \bmod M,1}}} \\ &= -1 + R_a(e_{j \bmod M,0} - e_{i,0}) - R_a(e_{j \bmod M,1} - e_{i,1}) \\ &= -1 + (-1) + 1 \\ &= -1 \end{aligned} \quad (8)$$

When $i = 2M, 0 \leq j \leq M-1$,

$$\begin{aligned} R_{S_i, S_j}(0) &= -1 + \sum_{t_1=0}^{2^m-2} (-1)^{a_{t_1+e_{i,0}}} - \sum_{t_1=0}^{2^m-2} (-1)^{a_{t_1+e_{i,1}} + a_{t_1+e_{j,1}}} \\ &= -1 + (-1) + 1 \end{aligned}$$

$$= -1 \tag{9}$$

When $i = 2M, M \leq j \leq 2M - 1,$

$$\begin{aligned} R_{S_i, S_j}(0) &= -1 + \sum_{t_1=0}^{2^m-2} (-1)^{a_{t_1+e_j \bmod M,0}} - \sum_{t_1=0}^{2^m-2} (-1)^{a_{t_1+e_j \bmod M,1}} \\ &= -1 + (-1) + 1 \\ &= -1 \end{aligned} \tag{10}$$

Therefore, it is concluded that the in-phase cross-correlation function value of any two sequences in the sequence set S is -1 , and condition 2 is satisfied.

The following proves that the sequences in the sequence set S are all shifted unequal. It is easy to see that the sequence S_{2M} and the rest of the sequences are shifted unequal. Let S_i and S_j be any two different sequences in the sequence set $S, 0 \leq i \neq j \leq 2M - 1,$ assuming that the two sequences are shifted equivalently, that is, $L^t(S_j) = S_i.$ Analysis of the following situations.

Case 1 When $0 \leq i \neq j \leq M - 1$ and $= 2t_1, 0 \leq t \leq 2^{m+1} - 2$ gives $0 \leq t_1 \leq 2^m - 1.$ The necessary and sufficient condition for $L^t(S_j) = S_i$ to hold is that the following equations hold simultaneously.

$$\begin{cases} a_{N-t_1+e_{i,0}} = 0 \\ a_{e_{j,1}+t_1+1} = 0 \\ a_{N-t_1+e_{i,1}} = a_{0+e_{j,0}} \end{cases} \tag{11}$$

When $0 \leq l \leq N - t_1 - 1,$

$$\begin{cases} a_{l+e_{i,0}} = a_{l+e_{j,0}+t_1} \\ a_{l+e_{i,1}} = a_{l+e_{j,1}+t_1} \end{cases} \tag{12}$$

When $N - t_1 + 1 \leq l \leq N - 1,$

$$\begin{cases} a_{l+e_{i,0}} = a_{l+e_{j,1}+t_1-1} \\ a_{l+e_{i,1}} = a_{l+e_{j,0}+t_1} \end{cases} \tag{13}$$

In other words, there is $L^t(S_j) = S_i$ if and only if the above formulas are simultaneously established. Divide the following cases to prove that the above formulas cannot be established at the same time.

When $0 \leq t_1 \leq 2^{m-1} - 2,$ observe that when $0 \leq l \leq N - t_1 - 2,$ all are established, and it is regarded as the sequence $a_{l+e_{i,0}}$ shift equivalent sequence of $L^{e_{i,0}}(a)$ is the first $N - t_1$ elements, $L^{e_{j,0}+t_1}(a)$ can be regarded as the first $N - t_1$ elements. From the shift-and-add characteristic of the m sequence, we know:

$$\begin{cases} L^{e_{i,0}}(a) + L^{e_{j,0}+t_1}(a) = L^k(a), e_{i,0} \neq e_{j,0} + t_1 \\ L^{e_{i,0}}(a) + L^{e_{j,0}+t_1}(a) = 0, e_{i,0} = e_{j,0} + t_1 \end{cases}$$

where $0 \leq k \leq N - 1$. In the above formula, 0 represents an all-zero sequence of length N . If $e_{i,0} \neq e_{j,0} + t_1$, it can be concluded that there is a zero run of length $N - t_1$ in the sequence $L^k(a)$. Because $L^k(a)$ is an m sequence, we know from Lemma 2 that the maximum run length of 0 in $L^k(a)$ is $L - 1 < 2^{m-1} - 1$, and because $N - t_1 \geq 2^{m-1} - 1$, it is obviously contradictory. So there are $e_{i,0} = e_{j,0} + t_1$, and similarly $e_{i,1} = e_{j,1} + t_1$ is established, and can be substituted into $i - j = t_1$ and $j - i = t_1$, and further $t_1 = 0$ and $i = j$ can be obtained. Contradicts with $i \neq j$, therefore, it is concluded that when $0 \leq t_1 \leq 2^{m-1}$, formula (12) does not hold.

When $2^{m-1} + 1 \leq t_1 \leq 2^m - 1$ and it is observed that $N - t_1 + 1 \leq l \leq N - 1$, all $e_{i,0} = e_{j,0} + t_1$ are established, and $a_{l+e_{l,0}}$ can be seen as $t_1 - 1$. As the shift equivalent sequence of the sequence $L^{e_{l,0}}(a)$, the end of the column a -prime, and is regarded as the end of element, from the shift additivity of the m sequence, we know:

$$\begin{cases} L^{e_{i,0}}(a) + L^{e_{j,1}+t_1-1}(a) = L^k(a), e_{i,0} \neq e_{j,1} + t_1 - 1 \\ L^{e_{i,0}}(a) + L^{e_{j,1}+t_1-1}(a) = 0, e_{i,0} = e_{j,1} + t_1 - 1 \end{cases}$$

4 Comparison of Construction Methods

This section compares and analyzes several construction methods of binary low-correlation zone sequence sets based on finite fields, and the obtained sequence set parameters are shown in Table 1.

It can be seen from Table 1 that this paper uses binary pseudo-random sequences to construct a class of optimal binary LCZ sequence sets. Compared with the previous

Table 1 Comparison of several binary LCZ sequence set construction methods

Method	Sequence set parameters	Initial sequence	Whether its optimal
Literature [2] method	$(2^n - 1, M, \frac{2^n-1}{2^m-1}, 1)$	GMW sequence	No
Literature [4] method	$(2^n - 1, 2^{m-1}, \frac{2^n-1}{2^m-1}, 1)$	Legendre sequence	No
Literature [13] method	$(2^n - 1, 2^m - 2^n, \frac{2^n-1}{2^m-1}, 1)$	Quadratic sequence	No
Proposed method	$(2^n - 1, 2^{m+1} - 1, \frac{2^n-1}{2^{m+1}-1}, 1)$	Binary pseudo-random sequence satisfying $L < 2^{m-1}$	Yes

method, the initial sequence selection of this method is more flexible. Different initial sequences can be selected to obtain different binary LCZ sequence sets, and the number of sequences obtained in the sequence set is larger, which can reach the theoretical limit. An example of a binary low-correlation zone sequence set is given below. Select the m sequence a (1001011) with a period of 7, and the function $h(x) = Tr_4^8(x)$ from the finite field F_{2^8} to F_{2^4} , and use the method in this paper to get the sequence Set 2 LCZ(255,15,17,1). In order to save space, it is expressed in hexadecimal notation. Among them, 0~7 are respectively as follows:

$$v_0 = (207332334712766342051332546137663420503305461376221$$

$$2050360156127622120723613571276220)$$

$$v_1 = (677670530102131413541462130740265652660357657127$$

$$3204741406146046647710543505326753102)$$

$$v_2 = (624503650015037160544430544152736315444401766067161$$

$$5772745333625204072733073216612416)$$

$$v_3 = (3050360130761220362660653551027320056342334714666$$

$$761055312566637753467507145020352041)$$

$$v_4 = (624005455601660210072361313165220320773433550237$$

$$5342563433703114265410513325647336635)$$

$$v_5 = (35624117656526062524502612270437154750754554073606$$

$$23066001323644310347557661101213754)$$

$$v_6 = (3545442132604355457727357217312240724100616464264$$

$$374244074512154330205767013450637163)$$

$$v_7 = (10553125646337535674045451201420411072361331761220$$

References

1. Gaudenzi RD, Elia C, Viola R (1992) Bandlimited quasisynchronous CDMA: a novel satellite access technique for mobile and personal communication system. *IEEE J Sel Areas Commun* 10(2):328–343
2. Long BQ, Zhang P, Hu JD (1998) A generalized QS-CDMA system and the design of new spreading codes. *IEEE Trans Veh Technol* 47(4):1268–1275
3. Tang XH, Fan PZ (2001) A class of pseudonoise sequence over GF(p) with low correlation zone. *IEEE Trans Inf Theory* 47(4):1644–1649
4. Jang JW (2007) New sets of optimal p-ary low-correlation zone sequences. *IEEE Trans Inf Theory* 53(2):815–821
5. Subbarao MV, Terlapu SK, Chakravarthy VVSSS, Satapaty SC (2021) Pattern recognition of time-varying signals using ensemble classifiers. In: *Microelectronics, electromagnetics and telecommunications*. Springer, Singapore, pp 725–733
6. Tang XH, Fan PZ (2003) Generalized d-form sequence and LCZ sequences based on the interleaving technique. In: *Proceedings of 7th iscta'03*. Ambleside, UK, pp 276–281
7. Kim YS, Jang JW, No JS et al (2006) New design of low-correlation zone sequence sets. *IEEE Trans Inf Theory* 52(10):4607–4616
8. Chung JH, Yang K (2008) New design of quaternary low-correlation zone sequence sets and quaternary Hadamard matrices. *IEEE Trans Inf Theory* 54(8):3733–3737
9. Tang XH, Fan PZ, Matsufuj I (2000) Lower bounds on the maximum correlation of sequence set with low or zero correlation zone. *Electron Lett* 36(6):551–552
10. Venkataramana S, Sekhar BVDS, Deshai N, Chakravarthy VVSSS, Rao SK (2019) Efficient time reducing and energy saving routing algorithm for wireless sensor network. *J Phys: Conf Ser* 1228(1):012002 IOP Publishing
11. Tang XH, Udaya P (2005) New construction of low correlation zone sequences form Hadamard matrices. In: *Proceedings of international symposium on ISIT 2005*, pp 482–486
12. Hu HG, Gong G (2010) New sets of zero or low correlation zone sequences via interleaving technique. *IEEE Trans Inf Theory* 56(4):1702–1713
13. Zhou ZC (2008) New families of binary low correlation zone sequences based on interleaved quadratic form sequences. *IEICE Trans Fundam* 91(11):3406–3409

Author Index

A

Abhishek, 205
Adepu Rajesh, 369
Adouthu Vamshi, 295
Ajeet Singh, 195
Akash Kumar Gupta, 235, 287
Aloy Anuja Mary, G., 265
Anuradha, T., 87
Appala Naidu Tentu, 195
Arif Ahmad Shehloo, 55
Ashoka Reddy, K., 353
Ashraf Alam, 1
Ashutosh Saxena, 153, 163, 195

B

Balaji, B., 361
Bonagiri Jyothi, 275
Bonthu Kotaiah, 67

C

Chandra Sekhar, M., 311, 321
Chowdary, P. S. R., 287

D

Dadi Ramesh, 379, 393
Darahasa, M., 87
Deepa, D., 75
Deepanshu, 205
Devika, K. D., 153
Duggirala Vijitendra, 33
Durgesh Kumar, 205

G

Ganesh, Reddy, 67
Govinda Rajulu, G., 75
Gunapreetham, A., 311

H

Hanu Vamshi, K., 339
Harshit Agrawal, 33
Helini, K., 329

I

Inapanuri Sucharitha, 295

J

Jamuna Rani, M., 75
Jishitha, N., 95

K

Kishan Rao, K., 413, 425
Komuraiah, B., 353
Kothandaraman, D., 379, 393

L

Lakshmi Narayanan, S., 171
Lakshmi Ramani, B., 95

M

Mahika Kamale, N., 87
Mahitha, P., 87

Manish Deshwal, 221
 Manish Pandey, 23
 Manoj Kumar Vaddepalli, 369
 Moghal Ajarvali, 257
 Muheet Ahmed Butt, 55
 Murali, K., 265

N

Naga Lakshmi, V., 275
 Navneet Bhargava, 213
 Neha, K., 311
 Nichenamtela Neeraj, 257
 Nirmaladevi, R., 413, 425
 Nirmalendu Kumar, 213
 Nithya, B., 33

P

Parag Kulkarni, 187
 Prachi Medline Ekka, 11
 Prasad, N., 339
 Prasanth, R., 171
 Prasuna, K., 265
 Praveenkumar, C., 67

R

Radhakrishna, D., 67
 Radhika G. Deshmukh, 75
 Raghunandan, K. R., 67
 Rajasanthosh Kumar, T., 75
 Rajashree Narendra, 45
 Rajendra Prasad, P., 329
 Ramadevi, B., 353, 361
 Ramesh Babu, B. S. S. V., 287
 Ramya, N., 87
 Ranganath Kanakam, 393
 Ravi Kumar, R., 379
 Reddy, V. V., 353
 Riya Yadav, 23
 Roopa, M., 245
 Rupali Kute, 11
 Rupa, V., 329

S

Sagar, K., 403
 Sai Varshini, B., 311
 Sallauddin Mohmmad, 379, 393
 Sandeep Kumar, 213
 Sandeep Kumar Panda, 127, 143
 Sanjay Kumar, 205, 213
 Santosh Kumar Sahu, 23
 Sarada Devi, Y., 245
 Saravanan, D., 117

Satheesh Kumar, M., 171
 Satish Babu, G., 105
 Satish Rama Chowdary, P., 235, 287
 Saumya Srivastava, 221
 Sd. Abeeunnisa, 339
 Shabana, 379
 Shaik Himam Saheb, 105
 Shaik Samreen Sultana, 321
 Shaik Sana, 95
 Sheshikala, M., 393
 Shubhangi V. Urkude, 117
 Shunmugavel, S., 171
 Siron Anita Susan, T., 33
 Sravya, T., 95
 Sreevardhan Cheerla, 257
 Sri Durga, N., 95
 Sri Lakshmi, T., 95
 Srinivasa Rao Nandam, 295
 Srinivasa Rao, Naarisetti, 67
 Srinivas, M., 339
 Srinivas, M. S. S. S., 287
 Srujan Raju, K., 171, 187
 Srujay, P., 339
 Subbareddy, V., 257
 Suneel Raja, M., 311, 321
 Suresh, E., 361
 Suthendran, K., 171
 Swathi, A. V., 287
 Syed Noor Mohammad, 257

T

Thirupathi, V., 403
 Tripti Sharma, 221
 Trupti Shripad Tagare, 45

U

Udit Mamodiya, 75
 Umamaheshwar Soma, 361

V

Vamshi Krishna, M., 235
 Varaprasada Rao, K., 127, 143
 Varaprasad Rao, M., 187
 Vijaya, A., 353
 Vikas Tiwari, 195
 Vinayak Jagtap, 187
 Vishal, G., 311
 Vodapalli Prakash, 303

Y

Yerra Maithri, 163