Algorithms for Intelligent Systems
Series Editors: Jagdish Chand Bansal · Kusum Deep · Atulya K. Nagar

Dinesh Goyal
Anil Kumar
Vincenzo Piuri
Marcin Paprzycki *Editors*

Proceedings of the Third International Conference on Information Management and Machine Intelligence

ICIMMI 2021

Springer

Algorithms for Intelligent Systems

This book series publishes research on the analysis and development of algorithms for intelligent systems with their applications to various real world problems. It covers research related to autonomous agents, multi-agent systems, behavioral modeling, reinforcement learning, game theory, mechanism design, machine learning, meta-heuristic search, optimization, planning and scheduling, artificial neural networks, evolutionary computation, swarm intelligence and other algorithms for intelligent systems.

The book series includes recent advancements, modification and applications of the artificial neural networks, evolutionary computation, swarm intelligence, artificial immune systems, fuzzy system, autonomous and multi agent systems, machine learning and other intelligent systems related areas. The material will be beneficial for the graduate students, post-graduate students as well as the researchers who want a broader view of advances in algorithms for intelligent systems. The contents will also be useful to the researchers from other fields who have no knowledge of the power of intelligent systems, e.g. the researchers in the field of bioinformatics, biochemists, mechanical and chemical engineers, economists, musicians and medical practitioners.

The series publishes monographs, edited volumes, advanced textbooks and selected proceedings.

Indexed by zbMATH.

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

Dinesh Goyal · Anil Kumar · Vincenzo Piuri ·
Marcin Paprzycki
Editors

Proceedings of the Third International Conference on Information Management and Machine Intelligence

ICIMMI 2021

Springer

Editors
Dinesh Goyal
Poornima Institute of Engineering
and Technology
Jaipur, Rajasthan, India

Anil Kumar
Poornima Institute of Engineering
and Technology
Jaipur, Rajasthan, India

Vincenzo Piuri
Università degli Studi di Milano
Milan, Italy

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

ISSN 2524-7565 ISSN 2524-7573 (electronic)
Algorithms for Intelligent Systems
ISBN 978-981-19-2064-6 ISBN 978-981-19-2065-3 (eBook)
https://doi.org/10.1007/978-981-19-2065-3

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

Preface

The third International Conference on **Information Management and Machine Intelligence (ICIMMI-2021)** was organized by Poornima Institute of Engineering and Technology, Jaipur, Rajasthan, India, on December 23–24, 2021.

ICIMMI conference is organized annually to provide a platform for academicians, researchers, scientists, professionals, and students to share their knowledge and expertise in the field of information management and machine intelligence. It also provides an interdisciplinary platform for researchers, practitioners, and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in these fields.

- We encourage researchers, young scientists and academicians in the field of machine learning as this has been contributed in a variety of ways to our daily lives. Even during the outbreak of the coronavirus disease (COVID-19) pandemic, information management and machine learning has played a vital role in fighting against it.
- Propose new technologies to share their experiences and discuss trends for recent development and strategies concerning information management and machine learning.
- Augment technocrats and academicians by presenting their original and productive information.
- Spotlight on pioneering issues at the international level by bringing together experts from different countries.

ICIMMI-2021 was educative with the brilliant knowledge of invited keynote speakers and ideas represented by young researchers. There will be a wide range of sessions being organized throughout the conference schedule. We would like to thank all the organizing staff, the members of the program committee, and the reviewers. They have worked very stiff to review papers with valuable recommendations for authors to improve their ideas.

Prospective authors from academia, as well as industry, have submitted their full papers in the conference ICIMMI-2021 which have not been yet submitted/published and that illustrate the research, surveying works, and industrial application in all disciplines of engineering for intelligence-based applications and automation activities, especially with the emergence of data analytics, AI, machine learning and deep learning network security using machine learning.

ICIMMI-2021 Highlights

ICIMMI-2021 was organized by Poornima Institute of Engineering and Technology, Jaipur, Rajasthan, India, on December 23–24, 2021.

ICIMMI-2021 has conducted ten sessions:

- Emerging Perspectives of WSN and Artificial Intelligence for IoT Applications.
- Emerging Challenges and Opportunities of Advanced Technologies and High-performance Computing for IoT and Image Processing
- Big Data Analytics, Data Mining, and Computational Intelligence
- Emerging Trends in the Internet of Things, Machine Intelligence, Big Data Analytics, and Cloud Computing
- Machine Learning and Big Data
- Artificial intelligence, Internet of Things ML/DL as a New Paradigm: Issues Opportunities and their Challenges
- Applications of Pattern Recognition and Deep Learning
- Data Analytics and IOT
- Artificial Intelligence and Machine Learning Techniques in Cybersecurity and Digital Forensics
- Intelligent computing in Multidisciplinary Engineering Applications.

The **Third International Conference on Information Management and Machine Intelligence (ICIMMI-2021)** has been a big success and proved to be very beneficial and informational for everyone. At this conference, we received a total of 217 papers including international and national authors.

There are ten technical sessions and five keynote speakers (international and national) conducted in ICIMMI-2021.

Jaipur, India — Dinesh Goyal
Jaipur, India — Anil Kumar
Milan, Italy — Prof. Vincenzo Piuri
Warsaw, Poland — Prof. Marcin Paprzycki
ICIMMI-2021

Contents

1 **Analysis and Comparison of Swarm Intelligence Algorithm in IoT: A Survey** 1
Shikha Jain and Mohit Agarwal

2 **Implementing Client-Side Encryption for Enforcing Data Privacy on the Web Using Symmetric Cryptography: A Research Paper** 9
J. David Livingston, E. Kirubakaran, and J. Immanuel Johnraja

3 **System to Analyze Electricity Consumption Using IoT and On-Demand Cloud CRM Salesforce** 17
Jasmine Narula, Sunil Kumar Jangir, Shatakshi Singh, Manish Kumar, Dinesh Goyal, and Vijay Kumar

4 **Stera—A College Enquiry Chatbot** 25
D. Renuka Devi, T. A. Swetha Margaret, and S. Deshma

5 **Mobile Image Analysis for Detecting Melanoma** 33
S. Gowri, R. Surendran, J. Jabez, and Senduru Srinivasulu

6 **Minimization of Power in Home Automation by IOT-Based Interactive Home** 45
Payal Bansal, Sandhya Sharma, and Pallavi Sapkale

7 **An Efficient Security Technique Using Steganography and Machine Learning** 53
Sohan K. Yadav, S. K. Jha, Uttam K. Sharma, Shashikant Shrama, Pratibha Dixit, Shiv Prakash, and Ved P. Tiwari

8 **An Efficient Model for IoT Security Using Adopted RSA** 59
Sohan K. Yadav, S. K. Jha, Sudhakar Singh, Uttam K. Sharma, Pratibha Dixit, Shiv Prakash, and Amisha Gangwar

9 **Robotic Process Automation in IT SOX Compliance** 65
K. Murugappan and T. Sree Kala

10 Analyzing the Impact of Nationwide Lockdown on Air Pollution Levels in Indian Cities—And What We Can Learn from It 73
Sanayya, Ahraz Ahmad Arfi, and Sherin Zafar

11 A Comparative Study of Time Series Models for Blood Glucose Prediction 81
Sofia Goel and Sudhansh Sharma

12 Machine Learning Approaches in Mobile Data Forensic: An Overview 93
Preeti Dudhe and S. R. Gupta

13 Generating an Extract Summary from a Document 103
Fatima Boumahdi, Ayoub Zeroual, Ibtissam Boulghiti, and Hamza Hentabli

14 Obtrusion Detection Using Hybrid Cloud Models 109
Siddarth Chaturvedi, Swati Jadon, and Ankush Sharma

15 Comparative Analysis of Speech Enhancement Techniques in Perceptive of Hearing Aid Design 117
Hrishikesh B. Vanjari and Mahesh T. Kolte

16 Smart Walking Stick: An Aid to Visually Impaired 127
Kritika Singh, Heemal Yadav, Kunal Aggarwal, and Garima Sharma

17 Hydroponic Farming as a Contemporary, Dependable, and Efficient Agricultural System: Overview 141
Hari Mohan Rai, M. K. Singh, A. N. Mishra, and Aman Solanki

18 Internet of Things: The Next Generation Internet 149
Shruti and Shalli Rani

19 GIS for Disaster Management: A System to Aid Users with Relevant Information 159
Shubham Aghav, Prashant Solanki, and Sushila Palwe

20 Recent Trends in E-Learning Using Web 4.0 167
Juhi Singh, Arun Kumar Singh, and Mukesh Singla

21 Dosimetry Effect of Flattening Filter Free Energy Beams in Prostate Malignant Cells in Intensity Modulated RT 175
Manjeet Kumar, Sunita Dahiya, and Sunil K. Chaudhary

22 Crop Disease Prediction Using Deep ConvNet Architecture Technique 187
Angshuman Roy, Deepthi Sehrawat, and Juhi Singh

23 High Dimensional Data Clustering Using Forward Feature Selection Framework for Medical Data 197
D. Karthika and K. Kalaiselvi

24 Artificial Intelligence (AI) Startups in Health Sector in India: Challenges and Regulation in India 203
K. Gagandeep, M. Rishabh, and Sonali Vyas

25 Analysis of Deep Learning Models for Security in IoT 217
Ankita, Himanshi Babbar, and Shalli Rani

26 Adobe Photoshop Vulnerabilities 229
Kanishca Goyal, Kopal Chaturvedi, and Mehak Khurana

27 Digital Information Management in Agriculture—Empirical Analysis 243
C. Ganeshkumar and Arokiaraj David

28 Power of Predictive Intelligence for Service Desk 251
Sonali Vyas and Abhimanyu Vyas

29 Visual Studio Vulnerabilities and Its Secure Software Development 259
Tanu Verma, Yukti Ghablani, and Mehak Khurana

30 Global Outlook of Cyber Security 269
Tripti Lamba and Shivani Kandwal

31 Consensus Mechanism Using Sharding Approach in Consortium Blockchain 277
Shivani Wadhwa, Divya Gupta, and Lipakshi

32 Education Through NGOs: Challenges and Opportunities 285
Sandeep Mathur and Riya Saini

33 Delay Efficient Caching in Fog Computing 293
Divya Gupta, Shivani Wadhwa, Shalli Rani, and Parth Sharma

34 Optimization and Pursuance Analysis of RDBMS for Relational Algebraic Operations—MySQL 299
Arpana Chaturvedi and Deepti Khanna

35 Chatbot Farming System 311
Tripti Lamba and Ritika Keshri

36 Smart Cities in Emerging Economies: Opportunities, Challenges and Policy Implications 319
Roli Raghuvanshi and Tanushree Sharma

37 AMSS: A Novel Take on Web Page Ranking 331
Yash Matta, Dheeraj Malhotra, and Neha Verma

38 Impact of COVID-19 Vaccination: A Machine Learning Approach 341
Ekata Gupta, Mukta Goyal, Abhishek Srivastava, and Anchal Pathak

39 Task Allocation in IoT: A Systematic Review of Techniques and Issues 357
Malvinder Singh Bali and Kamali Gupta

40 Healthcare BPM's Rebirth: A Case of Digital Disruption Post COVID-19 369
Pallavi Kudal, Sunny Dawar, Abhishek Sharma, and Prince Dawar

41 Recurrent Neural Network: A Flexible Tool of Computational Neuroscience Research 377
Akanksha Kaushik, Jyotsna Singh, and Shilpa Mahajan

42 Data Protection and Security in Affordable Home/Remote Monitoring (MCPS) of Patients 385
Sumit Saini, Shilpa Mahajan, and Mehak Khurana

43 Employee Emotions on Work from Home During COVID-19: Sentiment Analysis Approach 397
Aanyaa Chaudhary and Sonal Khandelwal

44 45 nm CMOS-Based MTSPC DFF Design for High Frequency Operation 409
Suman Bishnoi, Shubham Gupta, Deepak Bhatia, and Riyaz Ahmed

45 An Improved Convolutional Neural Network for Classification of Type-2 Diabetes Mellitus 417
Shatakshi Singh, Bhoomika Rathore, Harshita Das, Shalini Agrawal, Dawa Bhutia, Vinod Maan, Sunil Kumar Jangir, and Manish Kumar

46 Reviewing Fake News Classification Algorithms 425
Y. Arora and Sunil Sikka

47 A Review on Congestion Control Using Routing Technique and Machine Learning 431
S. Hassija, Y. Arora, K. Tripathi, and M. Vijarania

48 Detecting Disorders of Ophthalmology Using Artificial Intelligence-Based Deep Learning 445
R. Deepa and S. Vaishnavi

49 Collaborative Learning; A Case Study at Army Institute of Technology, Pune 451
Mridula Chandola, Nithya Basker, and Sachin Tanwade

50 Millimeter Wave SIW Antenna for 5G Application 463
T. A. Balarajuswamy and Nakkeeran Rangaswamy

51 Importance of Medical Instruments in Treating COVID Patients: A Case Study of Alwar District in Rajasthan 475
Arushi Saraswat

52 Sustainability Through Microfinance Among the Small Farmers of Kotdwar Bhabhar Region in Uttarakhand 485
Manisha Sarwaliya, V. M. Tripathi, and Ambica Prakash Mani

53 Animal Accident Prevention on Railway Tracks Using Convolution Neural Network 497
Sandeep Khatri and Jasraj Meena

54 Post-Pandemic Effect in Construction Industry in India and Its Remedial Measure 507
Mayank Dave and Deepanshu Solanki

55 Organic Modifiers—Chemically Modified Dimethyltindichloride Organic–Inorganic Hybrid Product: Design and Antimicrobial Activity 513
Komal Soni, Sanjiv Saxena, and Asha Jain

56 Wireless Power Transmission via Solar Power Satellite 523
Pinki Yadav, Mauviz Shahid, Harshit Singh, Sooraj Pandey, and Vishvajit Singh

57 A Review on Carpal Tunnel Syndrome Various Terminologies 533
Nikita Gautam and Amit Shrivastava

58 Deep Learning Approaches for DNA Transcription and Position of Genetic Factor of Bacteria—*Ralstonia solanacearum* 547
Mohseena Thaseen, Sari Luthfiyah, and M. M. V. Baig

59 Pervasive Review of Optic Biosensors-Based on Surface Plasmon Resonance and Its Development 557
Sandeep Kumar Jain, Garima Mathur, Yogesh C. Sharma, and Sandeep Vyas

60 Variability Analysis of Public Transit Bus Travel Time Using GPS Logs: A Case Study 567
B. P. Ashwini and R. Sumathi

61 Comparative Analysis of Waiting Delay Estimation Models for Signalized Intersections: A Case Study Tumakuru City 579
R. M. Savithramma and R. Sumathi

62 Effect of Different Fine Aggregate Materials in Mechanical Properties of Concrete 591
Muddana Surya Prasanth, Mahendrakar Hemanth Kumar, and Chadalawada Chandrasekhar

63 A Critical Analysis on Applications and Impact of Emerging Technologies in Employment and Skills Domain in e-Governance Projects 597
Yashpal Soni, Geeta Chhabra Gandhi, and Dinesh Goyal

64 Risk and Challenges in Intelligent Systems 607
Akshita Rastogi, Shivam, and Rekha Jain

65 1–4D Protein Structures Prediction Using Machine Learning and Deep Learning from Amino Acid Sequences 615
Atrakesh Pandey and Rekha Jain

66 Health Assistant Using Natural Language Processing 623
Shubham Singh Dagur, Pooja Sharma, and Rekha Jain

67 A Comparative Study of E-Learning Applications 635
Tanya Garg and Ruchi Goyal

68 Application of Ontologies in the Enterprise—Overview and Critical Analysis 647
Katarzyna Wasielewska-Michniewska, Maria Ganzha, Marcin Paprzycki, and Aleksander Denisiuk

Author Index 659

About the Editors

Dr. Dinesh Goyal is working as Principal at revered Institute, namely Poornima Institute of Engineering and Technology. Acquiring an experience of 20 years in teaching, and perceive keen interest in research area relating Cloud Security, Image Processing and Information Security. With a mission to append more and better skill set, has organized short term training programs as Convener and Co-Convener within during this short career span. He has been instrument in obtaining accreditations for his institutions, from various agencies like NAAC & NBA, He has received Grants for Research, Development, Conference & workshops worth Rs. 85 Lakh, from agencies like AICTE, TEQIP, etc. He has been awarded by "Elets Excellence Award 2017" at Higher Education & Human Resource Conclave by Higher Education Department of Government of Rajasthan. Under his leadership, Institutions has also excelled in Industry Academia Interface, has established centers with major tech giants like Microsoft, Google & Amazon, etc. He has six full published patents and one copyright under his name. He has successfully published six edited books with big publishing giants like Springer, Wiley, IGI Global, Apple Academic Press, Taylor & Francis and Eureka. He has published three SCI & 21 Scopus indexed papers & is editors of two SCI & five Scopus Indexed Journals, special issues. He has successfully guided eight Ph.D. Scholars & 31 PG Scholars. He has also attended more than 25 International Conferences & has been invited speaker for more than 15 Conferences & Seminars. He is life member of ISC & ISTE and fellow member of CSI & ISTE.

Dr. Anil Kumar has around 15 years of experience in teaching. He is currently working as an Associate Professor at Poornima Institute of Engineering & Technology (NBA and NAAC Accredited), Jaipur. Earlier he has worked at Sri Satya Sai University of Medical Sciences, Sehore, M. P & J. V. M. G. R. R. Institute of Computer Applications, Charkhi Dadri, Haryana. He has received a Ph.D. degree in the field of Computer Science & Engineering in 2013. He completed his M.Tech. degree with Distinction in Computer Science & Engineering from Guru Jambheshwar University, Hisar in 2005. He Completed his B.E. in Computer Science and Engineering from R. K. D. F. Institute of Science and Technology, Bhopal in 2002. His key areas of interest are Cybersecurity, Penetration Testing, Information Security, and cryptography. He has been a resource person in various FDP’s, workshops, guest lectures, and seminars. He has published many papers in various reputed National/International Journals and conferences. He has been a mentor to various M.C.A. & B.Tech. projects. He has also supervised Ph.D. students in the area of security, Green Computing. He has organized many events Like AICTE Training & Learning Program, Member of Organizing Committee of the Conference on ICIMMI 2019 & ICIMMI 2020 in collaboration with Springer.

Dr. Vincenzo Piuri has received his Ph.D. in computer engineering at Polytechnic of Milan, Italy (1989). He is Full Professor in computer engineering at the University of Milan, Italy (since 2000). He has been Associate Professor at Polytechnic of Milan, Italy and Visiting Professor at the University of Texas at Austin, USA, and visiting researcher at George Mason University, USA. His main research interests are: artificial intelligence, computational intelligence, intelligent systems, machine learning, pattern analysis and recognition, signal and image processing, biometrics, intelligent measurement systems, industrial applications, digital processing architectures, fault tolerance, cloud computing infrastructures, and internet-of-things. Original results have been published in 400+ papers in international journals, proceedings of international conferences, books, and book chapters. He is Fellow of the IEEE, Distinguished Scientist of ACM, and Senior Member of INNS. He is President of the IEEE Systems Council (2020–2021) and IEEE Region 8 Director-elect (2021–2022), and has been IEEE Vice President for Technical Activities (2015), IEEE Director, President of the IEEE Computational Intelligence Society, Vice President for Education of the IEEE Biometrics Council, Vice President for Publications of the IEEE Instrumentation and Measurement Society and the IEEE Systems Council, and Vice President for Membership of the IEEE Computational Intelligence Society. He has been Editor-in-Chief of the *IEEE Systems Journal* (2013–2019). He is Associate Editor of the *IEEE Transactions on Cloud Computing* and has been Associate Editor of the *IEEE Transactions on Computers*, the *IEEE Transactions on Neural Networks*, the *IEEE Transactions on Instrumentation and Measurement*, and *IEEE Access*. He received the IEEE Instrumentation and Measurement Society Technical Award (2002) and the IEEE TAB Hall of Honor (2019). He is Honorary Professor at: Obuda University, Hungary; Guangdong University of Petrochemical Technology, China; Northeastern University, China; Muroran Institute of Technology, Japan; Amity University, India; and Galgotias University, India.

Dr. Marcin Paprzycki is an Associate Professor at the Systems Research Institute, Polish Academy of Sciences. He has an MS from Adam Mickiewicz University in Poznań, Poland, a Ph.D. from Southern Methodist University in Dallas, Texas, and a Doctor of Science from the Bulgarian Academy of Sciences. He is a senior member of IEEE, a senior member of ACM, and was a Senior Fulbright Lecturer, and an IEEE CS Distinguished Visitor. He has contributed to more than 500 publications and was invited to the program committees of over 800 international conferences. He is on the editorial boards of 12 journals.

Chapter 1
Analysis and Comparison of Swarm Intelligence Algorithm in IoT: A Survey

Shikha Jain and Mohit Agarwal

1 Introduction

IoT is coined from two words, "Internet" and "Things." Internet connects the things to the many people in the network without inconvenience and the outcome is that it takes us further to the new lifestyle with new application such as autonomous vehicle [1], video surveillance [2], smart home, natural language processing and so on. IoT is a convergence of several new technologies that take part in the success of IoT. Devices connected to IoT includes sensors, actuators, smartphones, RFID tags, smart grids and so on [3], in such heterogeneous network of IoT where every application has different demand for the things attached to it, such as resource allocation, task scheduling, low density, low energy consumption and so on. Different objects/nodes of several features have to communicate with each other in the network so it must be ensured that the several resources are accessible to one another. Resource allocation and task scheduling are one of the issues in the IoT, especially when sensors and RFID tag are used. Usage of resources can be reduced by doing proper task scheduling; many researchers have proposed many algorithms to perform task scheduling for the improvement of network performance [4].

IoT establishes a relationship between real-life physical activities and virtual world. These days, many devices are associated with the Internet, and further, the quantities of such devices are increasing quickly [5]. So, to make resources available to these devices in very less time is the big challenge. In past few years, to get the optimized results, many advanced and latest algorithms have been proposed [6] by many researchers, and they proposed many swarm intelligence algorithms like

S. Jain
ABES Engineering College, Ghaziabad, U.P., India

S. Jain · M. Agarwal (✉)
Department of Computer Science and Engineering, Sharda University, Greater Noida, India
e-mail: rs.mohitag@gmail.com

D. Goyal et al. (eds.), *Proceedings of the Third International Conference on Information Management and Machine Intelligence*, Algorithms for Intelligent Systems,
https://doi.org/10.1007/978-981-19-2065-3_1

particle swarm optimization (PSO), cat swarm optimization [7], simulated annealing (SA), ant colony [8]. Individually, these algorithm does not produce better results; instead, hybridization of these algorithms gives better results. Discussion of different hybrid algorithm has been shown in the literature review, and comparison is shown in Table 1.

Table 1 Performance comparison of resource allocation and task scheduling technique in IoT

References	Author and year	Techniques	Objective	Results and accuracy
[4]	Ren et al. 2021	Hybrid optimization algorithm of SA and PSO	Low power consumption and lower the cost of allocating resources to the users	Increase performance by 2.6
[14]	Liao et al. 2020	PSO base meta-heuristic	Optimal cost for resource mapping in IoT environment	Achieved optimal cost as compared to techniques of SRA and DAG
[19]	Kong et al. 2019	Improved PSO and greedy algorithm	Minimize the execution time, use to arrange the task in order to their execution time from task basket and to find optimal routing solution	Optimal solution is obtained
[12]	Yang et al. 2019	Time and energy minimization scheduler (TEMS)	To decrease energy consumption and reduce execution time	Decrease energy consumption by 51.6%
[17]	Pradeep and Prem Jacob 2018	Harmony and cuckoo search algorithm (CHSA)	Reduce scheduling time in the cloud environment with multi-objective functions	CHSA gives better results compared to CS and HS
[20]	Prasanth et al. 2019	Hybridization of priority non pre-emptive algorithm and (ACO)	Decrease the task performing rate	Hybrid ACO gives better results compared to normal ACO
[21]	Shi and Zhang 2021	Clustering is used with ACO algorithm	Minimize the energy consumption and increase the network lifespan	Results shows that proposed algorithm is 50% more advanced than known algorithms

2 Swarm Intelligence Algorithms in IoT

Swarm intelligence (SI) algorithm is a simulation method to solve complex nonlinear problems inspired from social and biological behavior of numerous animals like fishes, ants, insects, flock and swarm [9]. The group behavior of these insects exhibits collective intelligence from their interaction (cooperation). SI, a kind of meta-heuristic algorithms, is the ability to handle large-scale and multi-objective problems in multidiscipline [10]. Though IoT is the dynamic and it is connected through several other advance developments like WSN, RFID, sensor technology connects physical objects to each other for communication and decision making. Still, there are many concerns to the researchers in the development of IoT due to its complex and dynamic behavior [11], and SI algorithms are investigated and modelled to compute such complex real-world optimization problems like routing resource management and task scheduling which are very common problems in IoT [12]. Scheduling refers to allocation of resources to several task on a single machine or many machines, and routing is to find best path, and the main goal is to reduce the computation time of the entire task. So, various SI algorithms like PSO, BCO, ACO with their variants [13] are used to solve the above-said problem.

3 Literature Review

The task allocation and resource utilization is the main challenge in the field of IoT for better energy consumption and low computation overheads. Several authors have proposed scheduling optimization algorithms to solve the said problems. Some of which are discussed as follows:

In [4], authors presented that individually SI algorithms like PSO and SA do not produce optimized results so they hybridized these two algorithm to get the better task allocation and resource utilization in the network of IoT, particle swarm optimization (PSO) and simulated annealing (SA). The challenges with PSO algorithm are that it does not produce optimized results in local environment and do not achieve the optimal response. So, the ultimate goal of this hybrid algorithm is to achieve low power consumption, minimizes the cost to allocating the resources to the user and reduce the task allocation time. Liao et al. [14] proposed a learning framework with service reliability, energy-aware and data backlog-aware aka SEB-GSI (global-state information) algorithm with CSI and SEB-UCB algorithm with single-MTD scenario and extended it to multi-machine with some optimization and matching theory. This hybrid combination of algorithm shows the improvement in throughput by 30% and 36% as compared with UCB. The dynamic cost model called TEMS is proposed in [15] authors have approached to limit energy utilization and processing time for allocating the resources to different IoT devices in the edge of different computing environments. Time and energy minimization scheduler (TEMS) scheduling algorithm chooses the suitable option, and results show that energy consumption is reduced by 51.6% and finish time of task is improved up to 86.6%.

In [16], the combination of ant colony optimization and cuckoo algorithm is presented for resolving the task scheduling problem. These algorithms (ACO and cuckoo) combine their best features to give a hybrid algorithm which performs better than the algorithms when applied individually. However, the constraint in ACO algorithm is that it can search in local domain due to which it does not obtain always optimized results. Harmony and cuckoo search algorithm does not exhibit better results individually, so to defeat the deficiencies of the discrete behavior of the Harmony and Cuckoo search author has suggested in [17] hybrid cuckoo search algorithm with harmony search algorithm (CHSA) and analysis represents that memory usage and energy consumption is less than the other approaches. In IoT, resource allocation with effective cost is required. So, in [18], particle swarm optimization (PSO)-based meta-heuristic algorithm is presented which is established in static environment only. Author achieved optimal cost in the multiple level of IoT network such as edge, node, cloud by multi-component application, although the scalability is the issue which is solved by disseminating the cloud load across edge devices such as routers and internet access devices.

In order to minimize the execution time for multiple robot task allocation (MRTA), Kong et al. presented in [19] combination of improved PSO and greedy algorithm (IPSO-G). Improved PSO is used to search combination of task in the network, and greedy algorithm is used to arrange the task from the task combination in order to their execution. After several iterations, optimal solution is obtained. This scheme is not good for local optimal solution with some special cases. Authors in their work [20], proposed the other approach of lowering the task completion rate of IoT based objects, which involves the combination of two algorithms, first is priority non pre-emptive algorithm to prioritize the tasks and second is Ant Colony Optimization (ACO) to find the shortest path. For low energy consumption, in [21], author approached clustering method to increase network life and control sensor node's energy consumption, and ACO algorithm was used to find optimal path for routing.

4 Application of SI Algorithms in IoT: An Overview

Nowadays, IoT is used almost everywhere which include smart homes, health care, autonomous vehicles, transportation smart city and water management. Various resources are used in IoT to perform such application, but IoT gadgets cannot perform complex issues because of their restricted battery. So, by applying SI algorithms, we can resolve many issues related to resource management. SI is the growing technique, which is the collective behavior of social insects. Swarm intelligence algorithm solves the problem related to self-learning, self-adoptability and creativity.

There is rapid development in transportations sector; autonomous connected vehicles share information with each other where optimized solution is a big challenge; SI-based ACO algorithms is the solution for finding the best path for information interchange, in which the group of ants use the phenomena to transfer the information to the others in the group to find the shortest path. Another application of SI-based PSO algorithm is used in hospitals to collect the patients information to monitor the health of particular patients by enhancing the multi-sensor frequency to measure body temperature, body fat, heart rate [22].

SI-based multi-objective PSO algorithm is used in cloud computing for optimized energy consumption for customer as well as cloud broker. PSO plays out its streamlining interaction to track down the best arrangements between the customers and the cloud brokers. It reduces the response time for clients and increase the profit of the cloud brokers [23]. Another IoT application is home energy management system (HEMS) where the most valuable resource is energy consumption as far as power cost decrease, SI-based grey wolf optimization (GWO) and bacterial foraging algorithm (BFA) methods enlivened by the idea of dark wolf and bacterium individually are used to find best optimal results [24]. Another SI-based cuckoo search algorithm is proposed for the smart homes to tackle the apparent light correspondence (VLC) power inclusion issues [25]. Basically, SI-based algorithms are used to find the best path in different environment; this application of SI algorithms is used in IoT.

5 Conclusion

In this paper, various swarm-based hybrid algorithms are discussed. It can be easy to conclude that hybrid algorithms are more efficient and outperforms the individual algorithms. SI applications give better results to find optimized results in centralized way, when there are so many constraints like scalability, sensors with less energy empowered and many more. With this advancement of technology, SI will assume a significant part to solve complex problems. This paper inspires the researchers and gives idea of combination of algorithms in producing better results beyond the current ones.

References

1. Krasniqi X, Hajrizi E (2016) Use of IoT technology to drive the automotive industry from connected to full autonomous vehicles. IFAC-PapersOnLine 49(29):269–274. https://doi.org/10.1016/j.ifacol.2016.11.078
2. Patil RM, Srinivas R, Rohith Y, Vinay NR, Pratiba D (2018) IoT enabled video surveillance system using Raspberry Pi. In: 2nd international conference on computational systems and information technology for sustainable solution, CSITSS 2017, pp 1–7. https://doi.org/10.1109/CSITSS.2017.8447877
3. Zhong RY, Dai QY, Qu T, Hu GJ, Huang GQ (2013) RFID-enabled real-time manufacturing execution system for mass-customization production. Robot Comput Integr Manuf 29(2):283–292. https://doi.org/10.1016/j.rcim.2012.08.001

4. Ren X, Zhang Z, Chen S, Abnoosian K (2021) An energy-aware method for task allocation in the Internet of things using a hybrid optimization algorithm. Concurr Comput 33(6):1–14. https://doi.org/10.1002/cpe.5967
5. Chopra K, Gupta K, Lambora A (2019) Future Internet: the Internet of Things—a literature review. In: Proceedings of international conference on machine learning, big data, cloud and parallel computing: trends, prespectives and prospects (COMITCon), pp 135–139. https://doi.org/10.1109/COMITCon.2019.8862269
6. Pradhan B, Vijayakumar V, Pratihar S, Kumar D, Reddy KHK, Roy DS (2021) A genetic algorithm based energy efficient group paging approach for IoT over 5G. J Syst Archit 113:101878. https://doi.org/10.1016/j.sysarc.2020.101878
7. Manshahia MS (2018) Swarm intelligence-based energy-efficient data delivery in WSAN to virtualise IoT in smart cities. IET Wirel Sens Syst 8(6):256–259. https://doi.org/10.1049/iet-wss.2018.5143
8. Daryanavard H, Harifi A (2019) UAV path planning for data gathering of IoT nodes: ant colony or simulated annealing optimization. In: Proceedings of 3rd international conference on internet of things and applications (IoT 2019), pp 1–4. https://doi.org/10.1109/IICITA.2019.8808834
9. Sun W, Tang M, Zhang L, Huo Z, Shu L (2020) A survey of using swarm intelligence algorithms in IoT. Sensors (Switzerland) 20(5). https://doi.org/10.3390/s20051420
10. Obagbuwa I (2018) Swarm intelligence algorithms and applications to real-world optimization problems: a survey. Int J Simul Syst Sci Technol. https://doi.org/10.5013/ijssst.a.19.02.05
11. Chakraborty T, Datta SK (2018) Application of swarm intelligence in internet of things. In: Proceedings of 2017 IEEE international symposium on consumer electronics (ISCE), pp 67–68. https://doi.org/10.1109/isce.2017.8355550
12. Yang J et al (2020) Swarm intelligence in data science: applications, opportunities and challenges. In: LNCS, vol 12145, no 2019. Springer International Publishing
13. Farzamkia S, Ranjbar H, Hatami A, Iman-Eini H (2016) A novel PSO (Particle Swarm Optimization)-based approach for optimal schedule of refrigerators using experimental models. Energy 107:707–715. https://doi.org/10.1016/j.energy.2016.04.069
14. Liao H et al (2020) Learning-based context-aware resource allocation for edge-computing-empowered industrial IoT. IEEE Internet Things J 7(5):4260–4277. https://doi.org/10.1109/JIOT.2019.2963371
15. Dos Anjos JCS, Gross JLG, Matteussi KJ, González GV, Leithardt VRQ, Geyer CFR (2021) An algorithm to minimize energy consumption and elapsed time for IoT workloads in a hybrid architecture. Sensors 21(9):1–20. https://doi.org/10.3390/s21092914
16. Babukartik R (2012) Hybrid algorithm using the advantage of ACO and cuckoo search for job scheduling. Int J Inf Technol Converg Serv 2(4):25–34. https://doi.org/10.5121/ijitcs.2012.2403
17. Pradeep K, Prem Jacob T (2018) A hybrid approach for task scheduling using the cuckoo and harmony search in cloud computing environment. Wirel Pers Commun 101(4):2287–2311. https://doi.org/10.1007/s11277-018-5816-0
18. Sharif M, Mercelis S, Marquez-Barja J, Hellinckx P (2018) A particle swarm optimization-based heuristic for optimal cost estimation in internet of things environment. In: ACM international conference proceeding series, pp 136–142. https://doi.org/10.1145/3289430.3289433
19. Kong X, Gao Y, Wang T, Liu J, Xu W (2019) Multi-robot task allocation strategy based on particle swarm optimization and greedy algorithm. In: Proceedings of 2019 IEEE 8th joint international information technology and artificial intelligence conference, ITAIC 2019, pp 1643–1646. https://doi.org/10.1109/ITAIC.2019.8785472
20. Prasanth A, George JA, Surendram P (2019) Optimal resource and task scheduling for IoT. In: 2019 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT 2019), pp 1–4. https://doi.org/10.1109/3ICT.2019.8910315
21. Shi B, Zhang Y (2021) A novel algorithm to optimize the energy consumption using IoT and based on ant colony algorithm. Energies 14(6):1–17. https://doi.org/10.3390/en14061709

22. Zedadra O, Guerrieri A, Jouandeau N, Spezzano G, Seridi H, Fortino G (2018) Swarm intelligence-based algorithms within IoT-based systems: a review. J Parallel Distrib Comput 122:173–187. https://doi.org/10.1016/j.jpdc.2018.08.007
23. Kumrai T, Ota K, Dong M, Kishigami J, Sung DK (2017) Multiobjective optimization in cloud brokering systems for connected internet of things. IEEE Internet Things J 4(2):404–413. https://doi.org/10.1109/JIOT.2016.2565562
24. Anwar ul Hassan CH, Khan MS, Ghafar A, Aimal S, Asif S, Javaid N (2018) Energy optimization in smart grid using grey wolf optimization algorithm and bacterial foraging algorithm. In: Lecture notes on data engineering and communications technologies, vol 8, pp 166–177. https://doi.org/10.1007/978-3-319-65636-6_15
25. Sun G, Liu Y, Yang M, Wang A, Liang S, Zhang Y (2017) Coverage optimization of VLC in smart homes based on improved cuckoo search algorithm. Comput Netw 116:63–78. https://doi.org/10.1016/j.comnet.2017.02.014

Chapter 2
Implementing Client-Side Encryption for Enforcing Data Privacy on the Web Using Symmetric Cryptography: A Research Paper

J. David Livingston, E. Kirubakaran, and J. Immanuel Johnraja

1 Introduction

Security is the major concern for all users accessing the Web. The Web needs to be secured as valuable information is stored on it. The Web is prone to different forms of attacks, which threats its security. An unauthorized user with malicious intention can threaten the integrity of information on the Web. He may try to connect to competitor's site and download information or business secrets from it. Therefore, it is the duty of every user of the Web to protect his/her valuable information on the Web by protecting the client, server, and the network—the three major components of World Wide Web (WWW). The client on the Web is the computer at the user end. On the client, the Web browser and the local system are at risk. The server is a remote computer on the Internet that hosts the Web server. The data on the server are prone to modification or damage by unauthorized users. The connection between the client and the server is also at risk because the data being transferred between the source, and the destination can be modified maliciously during transit. Hence, security mechanisms are of great importance because they ensure confidentiality and integrity of information on the Web. The basic security mechanism to ensure confidentiality of data on the Web is cryptography. Cryptography is the science of converting data that is in a readable form into an unreadable form. It is used to

J. David Livingston (✉)
Research Scholar, Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu, India
e-mail: davidlivingstonj@karunya.edu.in

E. Kirubakaran
Director, Grace College of Engineering, Thoothukudi, Tamil Nadu, India

J. Immanuel Johnraja
Associate Professor, Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamilnadu, India

D. Goyal et al. (eds.), *Proceedings of the Third International Conference on Information Management and Machine Intelligence*, Algorithms for Intelligent Systems,
https://doi.org/10.1007/978-981-19-2065-3_2

protect information from numerous risks and attacks on the communication medium between transacting parties. In this paper, the client-side encryption—a mechanism using which encryption of data at the client side before its migration onto the Web is discussed.

There are two types of cryptographic techniques, based on the keys used for encryption—symmetric and asymmetric. In symmetric cryptography, the receiver can decrypt the ciphertext using the same key with which the sender encrypted the plain text. On the other hand, in asymmetric cryptography, a pair of keys is used for encryption and decryption process. In this key pair, one key is public to both the sender and the receiver. The sender uses the public key to encrypt the plain text. The second key is private to the receiver with which the decryption of the ciphertext can be done. The following are the two major differences between the symmetric and the asymmetric-key cryptography:

i. The process of encryption and decryption is faster in symmetric cryptography as compared to that of asymmetric cryptographic algorithm.
ii. Key distribution is a big problem in symmetric-key encryption, whereas it is not at all a problem in asymmetric-key encryption algorithm.

Both types of encryption methods have advantages and disadvantages. Though the key management is a big issue in symmetric cryptography, the algorithm is easy to implement since it uses a single key for both encryption and decryption. It also works faster than that of the asymmetric cryptography. Thus, the symmetric-key encryption is recommended for use to encrypt data that are not supposed to be shared with others on the Web. In that case, nobody other than the owner of the data knows the key used for encryption. Thus, other people, without knowing the key, cannot read or modify confidential information stored on the Internet.

2 Client/Server Architecture of Web Application

2.1 Web Client and Web Server

Web browser is a client application that provides the interface using which a Web user can interact with the Web server for Web site navigation. Internet Explorer and Netscape Navigator are some of the commonly used Web browsers. A Web server, on the other hand, is a server application running on a remote machine. Web servers use protocols to enable communication over the Internet. Hyper-text transfer protocol (HTTP), file transfer protocol (FTP), and simple mail transfer protocol (SMTP) are some of the protocols used for the interaction between the Web server and the Web browser (Fig. 1).

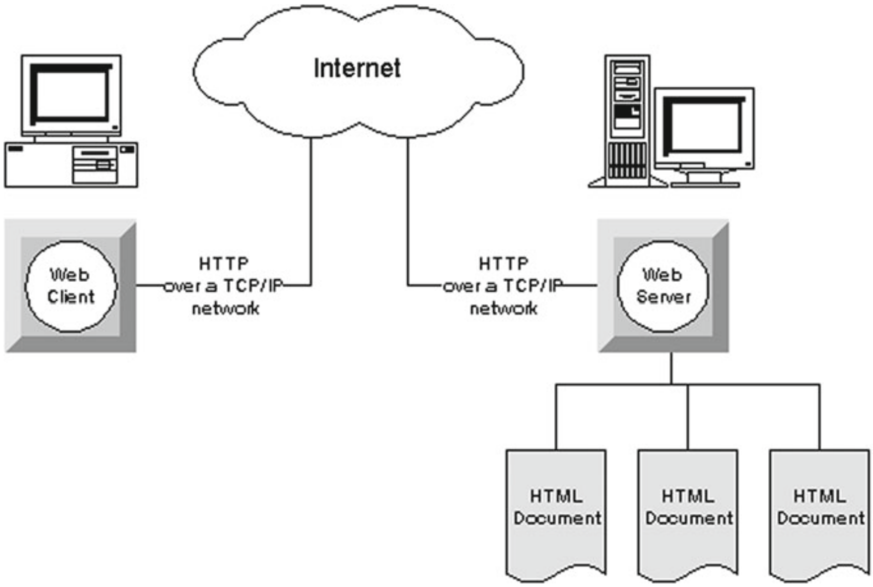

Fig. 1 Interaction between Web client and Web server on the Internet

2.2 Need for Securing the Confidential Data on the Web

The Web is prone to different forms of attacks that threaten its security. At the client side, the Web browser and the local system are at risk. The server, on the other hand, comprises the Web server. The data on the server are prone to modification or damage by unauthorized users. Hence, the confidentiality of data is of utmost importance when using the Web. Data confidentiality can be achieved by applying encryption on data that can be stored and retrieved from Web server. In this research, encryption of confidential data is scheduled to take place at the client side before their migration onto the Web for their storage at the server side.

3 Two Types of Research Approaches

There are three major steps involved in doing a research. They are as follows:

i. Formulation of research question
ii. Reviewing the existing literature and finding the research gap
iii. Articulate and enhance the research question and proposal to others in order to convince them.

A good research is systematic, and at the end, the data collected during the research support very strongly the statements, and the claims, or the arguments that the researcher put forth on the basis of collected data. Research approaches are plans and procedures that include various steps such as data collection, data analysis, and data interpretation. There are two major classification of research approach based on the methods used for collecting and analyzing the data to be handled in research. They are namely qualitative approach and quantitative approach.

3.1 Qualitative Approach of Research

Qualitative approach makes use of the following methods for data collection and interpretation:

- It makes use of emerging questions and procedures for data collection
- Data collection typically takes place in participant's setting
- Data analysis leads to the interpretation of the meaning of data being collected
- Finally, the qualitative research involves preparing the final written report.

3.2 Quantitative Approach of Research

Quantitative research involves the following steps for collecting and analyzing the data during the research process:

- It makes use of testing objective theories for finding the relationship among variables.
- Data are derived from instruments.
- Data analysis of numbered data is done with the help of statistical procedures.
- At last, the researcher has to prepare the final written report under various headings that include (a) Introduction, (b) Literature and Theory, (c) Methods, (d) Results, and (e) Discussion.

4 Securing Data on the Web

The Web is prone to different forms of attacks that threaten its security. At the client side, the Web browser and the local system are at risk. The server, on the other hand, comprises the Web server. The data on the server are prone to modification or damage by unauthorized users. Hence, the confidentiality of data is of utmost importance when using the Web. Data confidentiality can be achieved by applying encryption on data that can be stored and retrieved from Web server. In cryptography, the sender encrypts plain text into ciphertext by using a mathematical algorithm and a key value. Although the algorithm that a sender uses for encryption might be a general mathematical formula, the keys will be secret values known only to the sender and the receiver. The secrecy of keys prevents people other than the sender and the receiver from understanding the message, thus preventing unauthorized access on the critical data.

Cryptographic techniques can be classified broadly into two types: symmetric-key cryptography and asymmetric-key cryptography, based on the keys used for encryption. In symmetric-key encryption, single key is used for both encryption and decryption. The receiver can decrypt the ciphertext using the same key with which the sender encrypted the plain text. On the other hand, in asymmetric-key encryption, a pair of keys is used for encryption and decryption process. In this key pair, one key is public to both the sender and the receiver. The sender uses the public key to encrypt the plain text. The second key is private to the receiver with which the decryption of the ciphertext can be done. The following are the two major differences between the symmetric and the asymmetric-key cryptography:

i. The process of encryption and decryption is faster in symmetric cryptography as compared to that of asymmetric cryptographic algorithm.
ii. Key distribution is a big problem in symmetric-key encryption, whereas it is not at all a problem in asymmetric-key encryption algorithm.

Both types of encryption methods have advantages and disadvantages. Though the key management is a big issue in symmetric cryptography, the algorithm is easy to implement since it uses a single key for both encryption and decryption. It also works faster than that of the asymmetric cryptography. Thus, the symmetric-key encryption is recommended for use to encrypt data that are not supposed to be shared with others on the Web. In that case, nobody other than the owner of the data knows the key used for encryption. Thus, other people, without knowing the key, cannot read or modify confidential information stored on the Internet.

Kartit et al. [1] in their journal article identified two algorithms—AES and RSA for securing sensitive data on the cloud. AES is a kind of symmetric cryptography, whereas RSA is of type asymmetric cryptography. With the help of these two existing cryptographic algorithms, the authors proposed a new model for securing data on the cloud. In the proposed model, AES is used for encrypting the plain text, and RSA is used for encrypting the key used by AES. As per this model, plain text is encrypted using symmetric cryptography, and the key used for encrypting the plain text is encrypted using asymmetric cryptography. By applying both symmetric and asymmetric cryptography in encryption, both data as well as the key for encrypting the data are kept secret [2].

5 Client-Side Encryption of Data on the Web

The Internet provides remote access to resources such as storage and computation available worldwide. The virtual interaction of people on the Internet makes it difficult to recognize the identity of a person. In addition, the open-network structure of the Internet might allow third parties to read and change data in a communication over the network. Hence, every organization must maintain the integrity of data by preventing unauthorized modification. To secure confidential information on the Internet, one must put into practice necessary security measures.

Cryptography is a technique that helps to reduce security risks to the confidentiality and integrity of the data on the Internet. Moreover, the encryption of confidential data can be done either at the client machine (Web client) or on the server (Web server). The side (client/server) at which the encryption has to take place is decided based on the confidentiality of data to be protected. The critical data that need highest security in an organization are considered as in Level 1. In Level 2, we have information that is important but not critical as in Level 1. Level 3 comprises of data that are not important in the daily operations of an organization.

Among the three levels of confidentiality, data exist at Level 1 and Level 2 need encryption so that they can be kept confidential on the Web. As the data in Level 1 is both confidential and important, it must be encrypted at the client-side itself before their migration onto the Web. Whereas, data in Level 2 can be encrypted after their migration since the criticality of data in Level 2 is less compared to that of Level 1.

Encryption of data in the database (at the client side) must be done before moving the data to the remote database. For Level-1 data (having critical and important information), the standard symmetric encryption algorithm—advanced encryption standard (AES)—is suggested. For Level-2 data (having only important but not critical information), an extended play-fair algorithm is proposed [3]. Encrypting the data needs to be done for text files before they are uploaded onto the server. The key used for encryption must be kept secret in a local database for performing decryption process.

For encryption and decryption of text files at the client, either we can go for the standard algorithm like AES or an extended classical algorithm like extended play-fair algorithm. AES is the best option for securing the data which are more sensitive in nature. But, searching a sub-string is not possible when the data are encrypted using AES. This limitation of AES is overcome by using an extended play-fair algorithm, which is meant for encryption of less-sensitive data in a file or database.

The major difference between AES and the proposed extended play-fair algorithm is that the standard algorithm—AES is a block cipher, whereas the extended play-fair algorithm is a stream cipher. AES operates on a block of data (say 128 bits) at a time. But, the extended play-fair algorithm operates on individual character. It considers each and every word (sequences of characters that form a word in English) as a block during encryption. Hence, it allows the searching of encrypted text on the server word by word (word search). Moreover, it considers the ordinal position of each and every character in a single word as a key for encryption of plain text to ciphertext. This results in a polyalphabetic cipher that can map the same character that appears more than once in a word with two different ciphertext characters.

6 Conclusion

In this research, the authors have suggested client-side cryptography for securing data moving from the client onto the server. The scope of this research is to secure data that are stored in any one of the file formats that include text (txt), comma separated values (csv), or Excel Sheet (xls). secure non-sensitive data stored in the cloud database. As a solution to provide security at the client-side itself, it is found that the data which are important as well as critical (Level 1) must be encrypted using advanced encryption standard (AES), whereas data which are important but not critical (level 2) can be encrypted at the client side with the help of an extended play-fair algorithm so that searching is possible on the encrypted data on the server.

References

1. Sood SK (2012) A combined approach to ensure data security in cloud computing. J Netw Comput Appl. https://doi.org/10.1016/j.jnca.2012.07.007
2. Kartit Z, El Marraki M et al (2015) Applying encryption algorithm to enhance data security in cloud storage. Eng Lett
3. David Livingston J, Kirubakaran E. Implementation of extended play-fair algorithm for client-side encryption of cloud data. In: Part of the advances in intelligent systems and computing book series (AISC), vol 1167. Springer, Singapore
4. Ghosh AK (2003) Ethics and security management on the web. NIIT material. Prentice-Hall of India Private Limited
5. David Livingston J, Kirubakaran E (2019) Client/server model of data privacy using extended playfair cipher for SaaS applications on the cloud. Int J Innov Technol Explor Eng. https://doi.org/10.35940/IJITEE.j9274.088101, https://www.ijitee.org/wp-content/uploads/papers/v8i10/J92740881019.pdf
6. Arockiam L, Monikandan S (2013) Data security and privacy in cloud storage using hybrid symmetric encryption algorithm. Int J Adv Res Comput Commun Eng 2(8). ISSN (Online): 2278-1021
7. Arshad NH, Shah SNT, Mohamed A, Mamat AM (2007) The design and implementation of database encryption. Int J Appl Math Inform 1(3)
8. Alves PGMR, Aranha DF (2018) A framework for searching encrypted databases. J Internet Serv Appl. https://doi.org/10.1186/s13174-017-0073-0
9. Li M, Yu S, Ren K, Lou W, Hou YT (2013) Towards privacyassured and searchable cloud data storage services. IEEE Netw
10. Pedro PG, Aranha DF (2018) A framework for searching encrypted databases. J Internet Serv Appl 9(1). https://doi.org/10.1186/s13174-017-0073-0

Chapter 3
System to Analyze Electricity Consumption Using IoT and On-Demand Cloud CRM Salesforce

Jasmine Narula, Sunil Kumar Jangir, Shatakshi Singh, Manish Kumar, Dinesh Goyal, and Vijay Kumar

1 Introduction

Consumption of electricity in Indian homes has increased by three times since 2000. The fraction of households with electricity supply access rose up to 55% in 2001 and to more than 80% by the year 2017. In the year 2014, 90 units (kWh) of electricity per month were consumed by an average Indian household which could provide enough power to four tube-lights, four ceiling fans, a television, a small refrigerator, and small kitchen appliances with typical usage hours and efficiency levels in India [1]. It is the need of the hour to control the usage of electricity, but before controlling, we must know the appliance which uses most of the electricity so that either we can

J. Narula
Salesforce, Hyderabad, India

S. K. Jangir
Department of Computer Science and Engineering, Chandigarh University, Mohali, Punjab, India

S. Singh (✉)
Department of Computer Science and Engineering, School of Engineering and Technology, Mody University of Science and Technology, Lakshmangarh, Rajasthan, India
e-mail: shatakshisingh2k@gmail.com

M. Kumar
Department of Biomedical Engineering, School of Engineering and Technology, Mody University of Science and Technology, Lakshmangarh, Rajasthan, India

D. Goyal
Department of Computer Science and Engineering, Poornima Institute of Engineering and Technology, Jaipur, Rajasthan, India

V. Kumar
Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, New Delhi, India

D. Goyal et al. (eds.), *Proceedings of the Third International Conference on Information Management and Machine Intelligence*, Algorithms for Intelligent Systems,
https://doi.org/10.1007/978-981-19-2065-3_3