Advances in Intelligent Systems and Computing 1348

Paramartha Dutta
Abhishek Bhattacharya
Soumi Dutta
Wen-Cheng Lai *Editors*

Emerging Technologies in Data Mining and Information Security

Proceedings of IEMIS 2022, Volume 3

Springer

Advances in Intelligent Systems and Computing

Volume 1348

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing such as: computational intelligence, soft computing including neural networks, fuzzy systems, evolutionary computing and the fusion of these paradigms, social intelligence, ambient intelligence, computational neuroscience, artificial life, virtual worlds and society, cognitive science and systems, Perception and Vision, DNA and immune based systems, self-organizing and adaptive systems, e-Learning and teaching, human-centered and human-centric computing, recommender systems, intelligent control, robotics and mechatronics including human-machine teaming, knowledge-based paradigms, learning paradigms, machine ethics, intelligent data analysis, knowledge management, intelligent agents, intelligent decision making and support, intelligent network security, trust management, interactive entertainment, Web intelligence and multimedia.

The publications within "Advances in Intelligent Systems and Computing" are primarily proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

Indexed by DBLP, INSPEC, WTI Frankfurt eG, zbMATH, Japanese Science and Technology Agency (JST).

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).

Paramartha Dutta · Abhishek Bhattacharya ·
Soumi Dutta · Wen-Cheng Lai
Editors

Emerging Technologies in Data Mining and Information Security

Proceedings of IEMIS 2022, Volume 3

Springer

Editors
Paramartha Dutta
Department of Computer and System Sciences
Visva-Bharati University
Santiniketan, India

Abhishek Bhattacharya
Department of Computer Application and Science
Institute of Engineering and Management
Kolkata, West Bengal, India

Soumi Dutta
Institute of Engineering and Management
Kolkata, India

Wen-Cheng Lai
Department of Electronic Engineering
National Taiwan University of Science and Technology
Taipei, Taiwan

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-981-19-4675-2 ISBN 978-981-19-4676-9 (eBook)
https://doi.org/10.1007/978-981-19-4676-9

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

Foreword

Welcome to the 3rd International Conference on Emerging Technologies in Data Mining and Information Security (IEMIS 2022) which was held on 23–25 February 2022 in Kolkata, India. As a premier conference in the field, IEMIS 2022 provides a highly competitive forum for reporting the latest developments in the research and application of Information Security and Data Mining. We are pleased to present the proceedings of the conference as its published record. The theme this year is Crossroad of Data Mining and Information Security, a topic that is quickly gaining traction in both academic and industrial discussions because of the relevance of Privacy Preserving Data Mining (PPDM model).

IEMIS is a young conference for research in the areas of Information and Network Security, Data Sciences, Big Data and Data Mining. Although 2018 was the debut year for IEMIS, it has already witnessed significant growth. As evidence of that, IEMIS received a record 610 submissions. The authors of the submitted papers come from 35 countries and regions. Authors of accepted papers are from 11 countries.

We hope that this programme will further stimulate research in Information Security and Data Mining and provide practitioners with better techniques, algorithms and tools for deployment. We feel honoured and privileged to serve the best recent developments in the field of Data Mining and Information Security to you through this exciting programme.

Satyajit Chakrabarti
President of IEM Group, India
Chief Patron, IEMIS 2022
Kolkata, India

Preface

This volume presents proceedings of the International Conference on Emerging Technologies in Data Mining and Information Security IEMIS2022, which took place in the Institute of Engineering and Management in Kolkata, India, from 23 to 25 February 2022. The volume appears in the series "Advances in Intelligent Systems and Computing" (AISC) published by Springer Nature, one of the largest and most prestigious scientific publishers, in the series which is one of the fastest growing book series in their programme. The AISC is meant to include various high-quality and timely publications, primarily conference proceedings of relevant conference, congresses and symposia but also monographs, on the theory, applications and implementations of broadly perceived modern intelligent systems and intelligent computing, in their modern understanding, i.e. including tools and techniques of artificial intelligence (AI), computational intelligence (CI)–which includes Data Mining, Information Security, neural networks, fuzzy systems, evolutionary computing, as well as hybrid approaches that synergistically combine these areas–but also topics such as—multi-agent systems, social intelligence, ambient intelligence, Web intelligence, computational neuroscience, artificial life, virtual worlds and societies, cognitive science and systems, perception and vision, DNA and immune-based systems, self-organizing and adaptive systems, e-learning and teaching, human-centred and human-centric computing, autonomous robotics, knowledge-based paradigms, learning paradigms, machine ethics, intelligent data analysis, various issues related to "Big Data", security and trust management, to just mention a few. These areas are at the forefront of science and technology and have been found useful and powerful in a wide variety of disciplines such as engineering, natural sciences, computer, computation and information sciences, ICT, economics, business, e-commerce, environment, health care, life science and social sciences. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and worldwide distribution. This permits a rapid and broad dissemination of research results. It is indexed by DBLP, INSPEC, WTI Frankfurt eG, zbMATH and Japanese Science and Technology Agency (JST). All books published in the series are submitted for consideration in Web of Science. IEMIS 2022 is an

annual conference series organized at the School of Information Technology, under the aegis of the Institute of Engineering and Management. Its idea came from the heritage of the other two cycles of events: IEMCON and UEMCON, which were organized by the Institute of Engineering and Management under the leadership of Prof. (Dr.) Satyajit Chakrabarti.

In this volume of "Advances in Intelligent Systems and Computing", we would like to present the results of studies on selected problems of Data Mining and Information Security. Security implementation is the contemporary answer to new challenges in threat evaluation of complex systems. Security approach in theory and engineering of complex systems (not only computer systems and networks) is based on multidisciplinary attitude to information theory, technology and maintenance of the systems working in real (and very often unfriendly) environments. Such a transformation has shaped natural evolution in topical range of subsequent IEMIS conferences, which can be seen over the recent years. Human factors likewise infest the best digital dangers. Work force administration and digital mindfulness are fundamental for accomplishing all-encompassing cybersecurity. This book will be of extraordinary incentive to a huge assortment of experts, scientists and understudies concentrating on the human part of the Internet and for the compelling assessment of safety efforts, interfaces, client-focused outline and plan for unique populaces, especially the elderly. We trust this book is instructive yet much more than it is provocative. We trust it moves, driving per user to examine different inquiries, applications and potential arrangements in making sheltered and secure plans for all.

The Programme Committee of the IEMIS 2022 Conference, its organizers and the editors of these proceedings would like to gratefully acknowledge the participation of all reviewers who helped to refine the contents of this volume and evaluated conference submissions. Our thanks go to all respected Keynote Speakers: Prof. Seyedali Mirjalili, Prof. Md. Abdur Razzak, Prof. Rafidah Md. Noor, Prof. Xin-She Yang, Prof. Reyer Zwiggelaar, Dr. Vincenzo Piuri, Dr. Shamim Kaiser and to our all session chairs.

Thanking all the authors who have chosen IEMIS 2022 as the publication platform for their research, we would like to express our hope that their papers will help in further developments in design and analysis of engineering aspects of complex systems, being a valuable source material for scientists, researchers, practitioners and students who work in these areas.

Santiniketan, India — Paramartha Dutta
Kolkata, India — Abhishek Bhattacharya
Kolkata, India — Soumi Dutta
Taipei, Taiwan — Wen-Cheng Lai

About This Book

This book features research papers presented at the International Conference on Emerging Technologies in Data Mining and Information Security (IEMIS 2022) held at the Institute of Engineering and Management, Kolkata, India, on 23–25 February 2022.

Data Mining is a current well-known topic in mirroring the exertion of finding learning from information. It gives the strategies that enable supervisors to acquire administrative data from their heritage frameworks. Its goal is to distinguish legitimate, novel, possibly valuable and justifiable connection and examples in information. Information Mining is made conceivable by the very nearness of the expansive databases.

Information Security advancement is an essential part to ensure open and private figuring structures. Notwithstanding how strict the security techniques and parts are, more affiliations are getting the chance to be weak to a broad assortment of security breaks against their electronic resources. Network-intrusion area is a key protect part against security perils, which have been growing in rate generally.

This book comprises high-quality research work by academicians and industrial experts in the field of computing and communication, including full-length papers, research-in-progress papers and case studies related to all the areas of Data Mining, machine learning, Internet of Things (IoT) and Information Security, etc.

Contents

Data Science and Data Analytics

About the Editors

Dr. Paramartha Dutta is currently Professor in the Department of Computer and System Sciences in, Visva-Bharati University, Shantiniketan, India. He did Bachelors and Masters in Statistics from ISI, Kolkata, India. Subsequently, he did Master of Technology in Computer Science from ISI, Kolkata, India. He did Ph.D. (Engineering) from BESU, Shibpore, India. He is Co-author of eight authored books apart from thirteen edited books and more than 200 and 40 research publications in peer-reviewed journals and conference proceedings. He is Co-inventor of 17 published patents. He is Fellow of IETE, Optical Society of India, IEI, Senior Member of ACM, IEEE, Computer Society of India, International Association for Computer Science and Information Technology, and Member of Advanced Computing and Communications Society, Indian Unit of Pattern Recognition and AI—the Indian Affiliate of the International Association for Pattern Recognition, ISCA, Indian Society for Technical Education, System Society of India.

Dr. Abhishek Bhattacharya is Assistant Professor at Institute of Engineering and Management, India. He has completed his Ph.D. (CSE), BIT, Mesra. He is certified as Publons Academy Peer Reviewer, 2020. His research interests are data mining, cyber security, and mobile computing. She has published 25 conference and journal papers in Springer, IEEE, IGI Global, Taylor & Francis, etc. He has 3 chapters in Taylor & Francis Group EAI. He is Peer Reviewer and TPC Member in different international journals. He was Editor in IEMIS 2020, IEMIS 2018, and special issues in IJWLTT. He is Member of several technical functional bodies such as IEEE, IFERP, MACUL, SDIWC, Internet Society, ICSES, ASR, AIDASCO, USERN, IRAN, and IAENG. He has published 3 patents.

Dr. Soumi Dutta is Associate Professor at Institute of Engineering and Management, India. She has completed her Ph.D. (Engineering), IIEST, Shibpur. She received her B.Tech. (IT) and M.Tech. (CSE) securing 1st position (Gold medalist), from MAKAUT. She is certified as Publons Academy Peer Reviewer, 2020, and Certified Microsoft Innovative Educator, 2020. Her research interests are data mining, OSN data analysis, and image processing. She has published 30 conference and journal

papers in Springer, IEEE, IGI Global, Taylor & Francis, etc. She has 5 chapters in Taylor-&-Francis Group and IGI-Global. She is Peer Reviewer and TPC Member in different international journals. She was Editor in CIPR-2020, CIPR2019, IEMIS-2020, CIIR-2021, and IEMIS-2018 special issues in IJWLTT. She is Member of several technical functional bodies such as IEEE, ACM, IEEE, IFERP, MACUL, SDIWC, Internet Society, ICSES, ASR, AIDASCO, USERN, IRAN, and IAENG. She has published 4 patents. She has delivered more than keynote talks in different international conferences.

Dr. Wen-Cheng Lai has been working in the field of radio frequency circuits, analog IC integrated design, microwave antenna, computer, and communication for more than 20 years. He completed his Ph.D. from National Taiwan University of Science and Technology. He has authored/co-authored more than 200 SCI indexed journals and IEEE conference/EI papers. He received the Ph.D. degree from the National Taiwan University of Science and Technology. He is Assistant Professor at the National Yunlin University of Science and Technology. He also worked as Executive Director of China Radio Association, Assistant Professor of National Yunlin University of Science and Technology, Assistant Professor of National Penghu University of Science and Technology, and Director of AsusTek Computer Inc.

Computational Intelligence

Empowering Indian Citizens Through the Secure E-Governance: The Digital India Initiative Context

Alka Agrawal, Raees Ahmad Khan, and Md Tarique Jamal Ansari

Abstract In India, e-governance has progressed from the computerized system of government units to programmes that encompass the finer elements of governance, including the citizen-centric approach, responsiveness, and accountability. Lessons learned from prior e-Government programmes have helped to shape the country's advanced e-Government policy. Although policymakers have been persuaded to speed up the deployment of e-Government across the different bodies of government at the national, state, and municipal level, yet there is a need for preventative steps to minimize cyber-attacks. In other ways, cyber-security issues appear to be roadblocks to e-governance achievement. These challenges may include socio-economic, religious, and technological limits, as well as privacy and security implications. Despite the numerous obstacles and limits, the government is confident in its ability to overcome these obstacles and pave the road for the success of e-government. Different significant initiatives of e-governance, security issues-challenges, and prospects of e-governance in the Digital India context are discussed in this study.

Keywords Digital India · Web application · E-Governance · Cyber-security · Digital platform · Durable security

1 Introduction

The term "e-governance" is now becoming increasingly popular. We've been seeing e-governance all around the world. Since socio-economic concerns have become more prevalent, governments have begun to extend their management from top to bottom levels in order to address a variety of socio-economic, research and engineering, and other challenges through the extensive use of digital devices. In fact, both established and emerging economies around the world use a variety of technological technologies to make public administration more efficient, transparent, and

A. Agrawal · R. A. Khan · M. T. J. Ansari (✉)
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh 226025, India
e-mail: tjtjansari@gmail.com

P. Dutta et al. (eds.), *Emerging Technologies in Data Mining and Information Security*, Advances in Intelligent Systems and Computing 1348,
https://doi.org/10.1007/978-981-19-4676-9_1

responsible [1–3]. In the Indian scenario, which is one of the world's most democratic, based on demographics, as well as geographically dispersed countries; there is still a disparity in the use of government services among its huge population. Moreover, there are still concerns associated with the nation's socio-economic position, such as unemployment, economic hardship, education, wellbeing, banking, as well as business, to name a few. As a consequence, the Indian government has been introducing number of innovative approaches in order to address these issues with optimum e-governance through extensive use of electronic devices [4–7].

In the Indian economy, e-governance is viewed as a supplement to information security, with the main emphasis on e-service implementation and IT policy creation. Initiatives in the E-Governance structure component are significant for incorporating procedures as well as security protocols in various organizations and firms, in addition to providing important strategies. The domain of cyber-security governance is particularly demanding in the context of attaining India's sustainability targets since it must create a security IT strategy and assist the implementation of e-services to citizens. Different implementation models and pathways have been designed as methods to cover the current gaps in public developments, where numerous stakeholders are involved in the design of the E-Government procedure. In recent times of e-Governance, major stakeholders such as the Ministry of Electronics and Information Technology (MeitY) as well as the Government of India (GoI) have implemented a number of regulatory steps. These steps are critical for realizing the vision and goals of the Digital India initiative. The programme is regarded as one of the most important factors in achieving long-term growth [8].

For IT systems, especially Digital India, cyberspace security is critical. A security layer should be included in every e-governance initiative. The security component of any e-governance initiative should be considered during the design phase. The administration's cyber-security unit must play a key role in monitoring the initial design. With the advancement of technology as well as digitalization, the view of security has experienced a significant transition. Authorities must take further safeguards by incorporating different government-led steps to ensure the integrity of an important country's infrastructure [9–12]. The Government of India's main programmes, the National e-Governance Plan as well as Digital India, aim to provide smooth government operations as well as accountable and productive solutions free of security risks. In other words, the goal of Digital India's e-governance strategy effort is to offer real-time governance to everyone by ensuring easy, fast, and responsible delivery of public services.

The rest of the paper is systematized as follows: Sect. 2 discusses the different e-governance initiatives in India. Section 3 discusses the various security issues in the way of efficient e-governance. Section 4 discusses the ways to enhance the security durability for e-Governance services. Finally, Sect. 5 concludes the paper.

2 E-Governance Initiatives in India

At the central as well as state levels, there seem to be a plethora of e-Government initiatives presently. The National e-Governance Plan (NeGP) was developed by the Department of Electronics and Information Technology and Administrative Reforms and Public Grievances with the goal of making all public services available to the general public, ensuring efficiency, visibility, and serviceability of such services at reasonable costs in order to meet the basic requirements of the general public. Several e-governance initiatives have been made possible because of the NeGP. Some of the popular e-Governance initiatives are listed below in Table 1.

3 Security Issues in E-Governance

The implementation of an e-governance paradigm in India, and also on a worldwide scale, is fraught with difficulties. The real difficulty is figuring out how to create and sustain effective e-governance projects that provide residents with cutting-edge e-services. Nevertheless, developing an e-governance portal as a service delivery method is not as simple. Efficient e-governance initiatives cannot be implemented in a hurry. In the case of India, e-Governance must allow for increased access to information and sharing of information between the state and central governments. The following subsections discuss the different security challenges faced by the e-governance initiatives.

3.1 Usability

Usability is concerned with making services and applications simple to use. Usability is tied to security considerations since efforts to improve data security may reduce their usability. In the context of software development, usability also refers to how and by whom data will be used. As a result, usability necessitates a major focus on challenges of e-Governance confidence elicited by interactions among actors who govern, provide, or profit from the services. Usability issues in electronic procurement arise from national regulations requiring company intelligence reports or eSignature solutions [10]. Distinct health systems in eHealth have diverse record mechanisms, and even within these processes, different record-keeping systems may exist. There's also the issue of fully digitizing record-keeping systems and ensuring that professionals and patients understand how to operate them.

Table 1 Initiatives taken for e-Governance in India

S. No.	E-governance initiatives	Details
1	Digital India	The Government of India started the Digital India attempt to assure that all citizens have access to government services via the internet
2	myGov.in	myGov.in is a nationwide citizen participation platform where citizens may contribute ideas and participate in policymaking and governance discussions
3	Aadhaar	Aadhaar is a UIDAI-issued unique identity card that serves as verification of person and residence using biometric information. It can be used to deliver substantial advantages to Indian citizens. Aadhaar can be used to e-sign documents
4	UMANG	UMANG is a unified mobile application that gives users access to a variety of central as well as state public services, such as Aadhaar, Digital Locker, PAN, as well as Employee Provident Fund facilities
5	PayGov	PayGov is a secured and efficient electronic portal for government to citizen engagement that has been approved by the government. PayGov allows users to make online payments to any public or private bank
6	Digital Locker	Citizens can use Digital Locker to electronically store sensitive documents such as mark sheets, PANs, Aadhaar cards, and degree credentials
7	Mobile Seva	The goal of Mobile Seva is to deliver government services via smartphones and tablets. Numerous live applications are available in the m-App store that can be utilized to access different governmental facilities
8	e-Hospital-online registration framework (ORF)	It is an endeavour to make it easier for patients to schedule Out Patient Department (OPD) visits with public hospitals via the internet. A patient care, clinical services, and health record administration are all included in this architecture
9	DARPAN	It is an online application that may be used to track and analyse the progress of the state's important and rising initiatives. It allows for actual data on Key Performance Indicators (KPIs) of specified schemes/projects to be presented to top State Government and district administration officials

(continued)

Table 1 (continued)

S. No.	E-governance initiatives	Details
10	Common services centres 2.0 (CSC 2.0)	CSCs are being applied to encourage and assist the adoption of information systems in the nation's rural regions

3.2 Network Security

With the rise of electronic government, communications infrastructure security is becoming more important, and resilience to network assaults (access, manipulation, and denial of service) is critical [11]. Threats to information security (cyber-terrorist activity, cyberwarfare, blended attacks, and so on) are constantly evolving as weaknesses in both existing and newly acquired systems are uncovered, necessitating solutions to address those threats. Methods to maintain network security comprise firewalls as well as proxy to keep undesired individuals out, antivirus applications and Internet Security Solution packages, anti-malware, encoding as well as enhanced computer designs, etc.

3.3 Access Control

Individuals who crave to use sensitive data for malicious reasons will be interested in all technological systems containing it. As a consequence, permissions to such systems are required to prevent unauthorized access to the data held. Generally, access control has a broad meaning, encompassing everything from your automobile lock to one's payment card pin code. However, the primary function is to prevent unauthorized access [12]. The systems range from data sources of citizen details, medical histories, banking information, and agreements to control of facilities such as electricity, roadways, and terminals, and the implies of access control will primarily be online or physical (walls, vouchers, tamper protective devices) in the space of electronic government.

3.4 Identification

The problem of identification poses a number of pertinent questions in current situations. The issue of validating a business's identification in technological capability is vital not only for ensuring that the business is who it claims to be when completing a contract, as well as in the long run. Issues have been expressed about the reliability of biometric information and whether it would be secured against fraudsters attempting to falsify the data and biometric passports. As a result, the efficacy of biometric data

would be a topic of discussion. The topic of how patients, physicians, and other medical professionals would recognize themselves in the e-healthcare environment is a challenge.

3.5 Interoperability

The potential of systems or operational processes to collaborate to accomplish a common goal has long been a goal in developing as well as even developed nations. The ability of the products they use to share and exchange data is required for effective interaction among government, industry, and individuals. The ineffectiveness of the electronic government system will be harmed by a lack of interoperability caused by language, a poor infrastructure, and diverse classification approaches.

4 Enhancing Security Durability for e-Governance Services

Given the country's growing IT sector, aggressive ambitions for rapid modernization and equitable progress, and India's significant impact on the worldwide IT market, putting the proper kind of emphasis on developing a safe computing platform with sufficient trust as well as assurance in online transactions, applications, operations, devices, and infrastructure became one of the nation's most pressing issues. Such planning is based on the country developing an appropriate cyber-security environment that is compatible with the globally distributed system.

The digital world is susceptible to a wide range of tragedies, whether deliberate or unintentional, man-made or environmental, and data transferred in virtual worlds can be used for malicious ends by both country and anonymous actors. Secure cyberspace is defined by the protection of personal information architecture and the restoration of data's confidentiality, integrity, and availability. Application security durability is often expressed as the software's expected serviceability. Since new security threats emerge every day, the requirement for software updates grows as time passes. If these risks become active, security will be compromised, and the application will malfunction as a consequence. The security durability properties have already been recognized and categorized by the authors. Figure 1 shows several security durability traits [13, 14] that should be significant to maximizing security durability, comprising dependability, trustworthiness, as well as human trust in order to empower Indian citizens with efficient e-Governance initiatives.

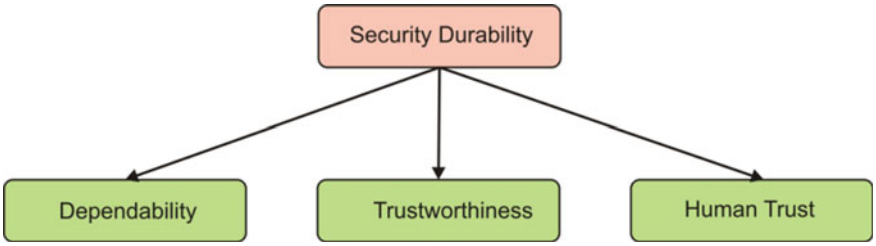

Fig. 1 Different factors of security durability

4.1 Dependability

The degree to which stakeholders believe a crucial system is referred to as dependability. The most significant system feature of a crucial system is generally dependability. To be effective, a system does not need to be recognized. The user's faith in the product's capacity to function normally is reflected in its dependability. Due to dependable software frequently necessitates certification, both procedure and product documents must be created. A prior requirements elicitation is also necessary to identify needs and requirements incompatibilities that could jeopardize the system's stability and security. This is at odds with the agile approaches of co-developing requirements and systems while minimizing paperwork. The agile approach, test-first progression, and user interaction in the development team are all strategies that can be included in an agile approach. Agile approaches can be employed as long as the software development group follows the procedure and logs their activities. However, because more documentation and preparation are required for trustworthy system design, "pure agile" is unfeasible.

4.2 Trustworthiness

The extent to which the system is supposed to work as intended in the presence of emerging interruptions, loss of execution completeness and consistency, human mistakes, system malfunctions, and cyber-attacks are referred to as trustworthiness. The accuracy of results one has in this anticipation is referred to as confidence of trustworthiness. For a business enterprise to have faith in a system, it must be proven to be trustworthy. Only purposeful process improvement for the construction of the solution at every level can ensure software's trustworthiness. A firm's ability to balance opposing aspects and provide the requisite performance all through the lifecycle from start to the finish is based on objective, clearly specified, quantifiable criteria and their prioritization. This specifies the expected level of quality, as well as how it would be maintained and controlled throughout the software engineering

and assurance testing processes. It is frequently necessary to consider who produced and administered the programme, as well as how this happened.

4.3 Human Trust

Human trust is generally described as a critical matter in which the person or group has an ethical value to the receiving entity in human–human contact. Customer experience in software producers is referred to as human trust in software. Whenever it comes to software, users' trust is based on the product's security architecture and the assurance that it will perform properly and protect their confidential information and data. Digital devices can be networked everywhere and at any time due to significant advancements in wireless networking technology. While travelling, these gadgets' apps dynamically identify hosts and resources with which they can initiate connections. However, the concern of being exposed to potentially dangerous transactions involving unknown parties may stymie interaction. An innovative approach towards the establishment of trust-based interactions is required to reduce this vulnerability.

5 Conclusion

Numerous policy initiatives and infrastructure improvements have been devoted to developing administration and support facilities in order to encourage e-Governance holistically in India. This article examined concerns linked to information security in e-governance, such as risks, attacks, and susceptibility, as well as success variables that may affect the number of threats, challenges, and weaknesses in the e-governance system in the context of the Digital India Initiative. The researcher believes that robust cyber-security practices must be used to enhance the confidentiality of e-government systems. Security measures, methods, and protocols, as well as the usage of access control, must be established in order to protect e-government platforms prevent the attack. This study also indicates that having a proper infrastructure that provides the required standard of durable security authentication, as well as having a continuous information security awareness programme to ensure that people are concerned about the security consequences, comprehend how to identify possible problems, and continue to maintain a secure e-government platform, are significant considerations.

Acknowledgements The authors gratefully acknowledge the support from Council of Science and Technology, Uttar Pradesh (UPCST); Letter No. CST/D-2300.

References

1. Y. Goswami, A. Agrawal, A. Bhatia, E-Governance: a tendering framework using blockchain with active participation of citizens, in *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (IEEE, December, 2020), pp. 1–4
2. B. Warf, Urban informatics and e-governance, in *Handbook of Urban Geography* (Edward Elgar Publishing, 2019)
3. M. Roy, E-Governance in the age of globalization: challenges ahead for India. SOCRATES **5**(3 and 4) (2017); September and December, 5, 88 (2018)
4. S. Sen, S. Mukhopadhyay, S. Karforma, A blockchain based framework for property registration system in e-governance. Int. J. Inf. Eng. Electron. Bus. **13**(4) (2021)
5. M.T.J. Ansari, D. Pandey, M. Alenezi, STORE: security threat oriented requirements engineering methodology. J. King Saud Univ. Comp. Inf. Sci. (2018)
6. M. Shah, E-governance in India: dream or reality. Int. J. Educ. Develop. ICT. **3**(2) (2007)
7. P. Malik, P. Dhillon, P. Verma, Challenges and future prospects for e-governance in India. Int. J. Sci. Eng. Technol. Res. **3**(7), 1964–1972 (2014)
8. V. Shubha, Deploy right, develop right: analysis and recommendation on using e-governance competency (EGCF) framework for digital India, in *Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance* (March, 2017), pp. 39–42
9. P. Rossel, M. Finger, Conceptualizing e-governance, in *Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance* (December, 2007), pp. 399–407
10. M. Bhuvana, S. Vasantha, Assessment of rural citizens satisfaction on the service quality of common service centers (CSCs) of e-governance. J. Crit. Rev. **7**(5), 302–305 (2020)
11. R. Kumar, M. Alenezi, M.T.J. Ansari, B.K. Gupta, A. Agrawal, R.A. Khan, Evaluating the impact of malware analysis techniques for securing web applications through a decision-making framework under fuzzy environment. Int. J. Intell. Eng. Syst. **13**(6), 94–109 (2020)
12. R. Betala, S. Gawade,.Usability analysis of e-governance applications, in *International Conference on Advanced Informatics for Computing Research* (Springer, Singapore, December, 2020), pp. 637–648
13. R. Kumar, M. Zarour, M. Alenezi, A. Agrawal, R.A. Khan, Measuring security durability of software through fuzzy-based decision-making process. Int. J. Comput. Intell. Syst. **12**(2), 627–642 (2019)
14. T.J. Ansari, D. Pandey, An integration of threat modeling with attack pattern and misuse case for effective security requirement elicitation. Int. J. Adv. Res. Comp. Sci. **8**(3) (2017)

A Performance Evaluation of Genetic Algorithm and Simulated Annealing for the Solution of TSP with Profit Using Python

Neha Garg, Mohit Kumar Kakkar, Gourav Gupta, and Jajji Singla

Abstract The Traveling Salesman Problem with profit (TSPP) is defined on an graph $G = (V, E)$. Traveling salesman problems with profit (TSPP) is a generalization of the traveling salesman problem (TSP), with one condition that it is not required for a sales person to travel all cities of the network. Our main purpose is to optimize the total profit and cost of the traveling. Here we are focusing on that in the case of TSPs; in real world scenario it is not always relevant for the salesman to visit each and every customer or city. To solve the problem, a GA with special mutation operators has been presented. Here we have utilized and compared different heuristic techniques genetic algorithm (GA) and simulated annealing (SA). Numbers of tours plots are generated for the comparison of performance of both the algorithm implemented for the solution of TSPP. These plots are beneficial for route planner and for those who want to apply this concept of TSPP. It has been observed that SA performs better than GA, as the response consumed less time than GA.

Keywords Genetic algorithm (GA) · Simulated annealing (SA) · Traveling salesman problems with profits (TSPP) · Python

1 Introduction

Let $G = (V, E)$ be an undirected graph with sets $V = \{v_1, v_2, v_3, \ldots, v_n\}$ of n vertices (cities) and $E\{e_1, e_2, \ldots\}$ of edges between vertices of graph. Let profit P_i be associated with each vertex $v_i \in V$ and a distance c_{ij} (cost) be associated with each edge between two vertices. In the recent years Nature inspired algorithm for optimization have progressively attracted the interests of many researchers, such as GA, ACO, particle swarm optimization (PSO), SA. All these nature inspired

N. Garg · M. K. Kakkar (✉) · G. Gupta · J. Singla
Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India
e-mail: mohit.kakkar@chitkara.edu.in

G. Gupta
e-mail: gourav.gupta@chitkara.edu.in

P. Dutta et al. (eds.), *Emerging Technologies in Data Mining and Information Security*, Advances in Intelligent Systems and Computing 1348,
https://doi.org/10.1007/978-981-19-4676-9_2

algorithms playing important role in solving NP hard type problems like TSP. TSP is considered as an NP hard problem, because, for a large number of cities or customers, it is not possible to find every optimized route under feasible time limit. Consequently, TSPs are well suited to solving using randomized optimization algorithms. In this study we are focusing on TSPP, traveling salesman problem with profit. The TSP is very popular studied problems in tour cost minimization and also it has the flavor of variety of applications as described by Erol and Bulut [8]. Similarly Hashim and Ismail [15] gave the applications of Traveling Salesman Problem in Tourist Visit in Langkawi. Iscan and Gunduz [17] provided an application of beautiful fruit fly algorithm for the solution of TSP. Xu et al. [29] studied the application of genetic algorithms (GA) on TSP. Raman and Gill [25] gave the Review of different heuristic algorithms (HA) on solving TSP. Almufti et al. [1] explained an ACO for Solving Symmetric TSP. Liu and Li [21] discussed a method called Greedy permuting for solution of traveling salesman problem based on GA.

Hacizade and Kaya [14] provided the concept which was on GA-based TSP solution and also explained the application of TSP for transport routes optimization. Kaspi et al. [19] discussed the approach for maximizing the profit per unit time for the TSP problem. Ayon et al. [3] discussed the novel algorithm Spider monkey optimization (SMO) to solve TSP. Ha, et al. [16] provided the min-cost TSP with drone. An application of improved ACO was given by the Yang and Wang [30] for traveling salesman problem. Zhang et al. [31] discussed the problem related to the TSP with profits for stochastic customers. Namazi et al. [23] provided the concept of profit guided heuristic for traveling problems, which was basically the combination of two concepts, TSP and knapsack problem (KP). Santini et al. [26] explained the approach of Heuristic and ML to TSP with Crowdsourcing. Qin et al. [24] solved the TSP with profits under time dependent cost (TDC) and multiple tour mode. Bouziaren and Aghezzaf [5] explained An Improved method of Branch-and-Cut for the solution of the TSPP. Gelareh et al. [12] discussed the new concept of draft limits for the solution of traveling salesman problem. Beraldi et al. [4] discussed about risk-averse TSPP. Lahyani et al. [20] explained the metaheuristic algorithm for solving multi-constrained TSPP. For the easiness they have assumed that service time included in the traveled duration. Gansterer et al. [11] discussed the MVPPD problem which is based on profitable multi-vehicle delivery problem. Eskandari et al. [9] provided a modified and enhanced ant colony optimization algorithm (ACO) for TSP. Yang and Wang [30] demonstrated an application of improved ant colony optimization algorithm on traveling salesman problem.

Costa et al. [6] presented a heuristic approach for TSP based on Christofides's heuristic. Filippi and Stevanato [10] studied the two-phase method for bi-objective combinatorial optimization problems.

Angelelli et al. [2] presented a new approach for solving TSP with profits (TSPP). Gottlieb et al. [13] presented an approach where total focusing on the prizes cities or customers where salesman decides that where he should visit with respect to the benefit of prizes. Kang et al. [18] delivered an algorithm which is based on time dependent profit. Derya et al. [7] proposed a new approach based on mixed integer programming for solving SGTSP. Mathur et al. [22] discussed a new strategy for the

Table 1 Summary of TSP with profits

Problem detail	Objective function based on	Constraints	Servers/Repairman/Salesman
Orienteering problem (OP) (selective TSP, maximum collection problem (MCP))	Maximize P (where P = profit)	Route duration	Single
Profitable route/tour problem (PTP)	Maximize $(P - C)$	NA	Single
Profit collecting traveling repairman problem (TRP)	Minimize C (where C = cost)	Route profit	Single
Team OP (TOP) (maximum profit based problem on multiple tour)	Maximizing P (where P = profit)	Route duration	Multiple

solution of (SA) Sales Augmentation using algorithm based on TSP and policy of Time Bound Marginal (TBM) Discount. Valdez et al. [28] discussed the comparison of Ant colony optimization with GA and SA also for the solution of TSP problem. Sarin et al. [27] discussed the multiple TSP with and without effect of precedence constraints.

In this paper, we will take care of the sales representative issue with benefits where the sales representative gathers some benefit for visiting each customer. As contradicted to the traditional TSP, there is no prerequisite to visit all the clients. The target of TSPP is to decide the best subset of clients to be visited in order to expand the all-out net benefit, which is equivalent to the all-out benefit earned from visited clients less the absolute expense of the visit. The last can be taken as the complete length of the visit determined as the Euclidean separation.

In Table 1 we summarize the classification of different kind of problems based on TSP and their characteristics.

2 Mathematical Modeling

A complete graph G: (V, E) is given where V = set of customers/cities including depot and E is the set of edges. For any subset S of V, we define $X^+(S) = \{(i, j):i \in S\}$. Traveling cost and time $(c_{ij}, t_{i,j})$ both may be associated with every edge $(i, j) \in E$. A profit p_i which is (a positive value may also zero) is fixed with each customer i which can be collected one time maximum.

The traveling time $t_{i,j}$ is connected with each edge $(i, j) \in A$. single salesman is present here at the depot with $T_{\max}$ Which is the maximum time limit associated with salesman for his journey.

Let us introduce the problem variables: