Computers and Electrical Engineering 99 (2022) 107786

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Guest Editorial: Introduction to the special section on security and privacy in the big data era (VSI-spbd)

1. Background

There is a rising need to secure data in the era of big data. But with the rapid development of technologies such as IoT and cloud computing, users' security and privacy measures are under tremendous pressure. Big data has led the world to an inflection point in machine learning and analytics, where powerful software tools are able to analyze vast amounts of information and often make better decisions than humans can. A major challenge for preserving privacy in the big data era is that it is hard to anonymize data without losing valuable information. Furthermore, big data has huge potential as a force for good, but numerous security and privacy concerns will dramatically reshape how big data is governed in the years and decades to come. Security, privacy, and related issues have become critical because of the wide applications in many areas.

The future of research on security and privacy in the big data era has infinite possibilities. It will focus on the particular features that have been used, leading to an increased understanding of privacy. This special section certainly acts as a concrete foundation as we are venturing into the big data era by exploring detailed information about the technologies and other influential factors that contribute to security and privacy issues in big data applications. It further examines the security and privacy issues that may arise as personal information moves increasingly through public channels, and new forms of analysis shed light on previously hidden patterns of behavior. It also highlights several opportunities for achieving transparency, accountability, and redress in the emerging big data landscape.

2. Papers in this special section

The response to this special section was overwhelming. Out of 27 submissions, ten were accepted for publication after a careful review process. Each paper was selected for inclusion in after a review process by three or more experts in the corresponding domain. The selected articles provide in-depth solutions to various security and privacy issues and challenging problems related to the big data era. Following is a brief description of the accepted papers.

In the paper by Nguyen et al. [1], the authors describe a collaborative approach for earlier detection of the IoT botnets. The authors stress the rapid growth of cyber attacks with the prevalence of big data. The proposed collaborative machine learning approach efficiently detects the IoT botnets at the earliest stage and prevents the probability of security threats across the IoT platform.

In the paper by Mohammed et al. [2], a Machine Learning-Assisted Cloud Computing Model (ML-CCM) approach is proposed to prevent the growing security threats across the cloud computing environment. It addresses various security issues relating to the diversity and complexity of the data across cloud computing platforms. The experimental results provide better data management capabilities and improved accuracy measures.

In the paper by Panda et al. [3], the authors propose a secure and lightweight authentication protocol for machine-to-machine communication in the context of industry 4.0. The objective of this work is to enhance the decision-making process of real-time data with improved security measures. This approach prevents security threats such as man-in-the-middle attacks, modification attacks, impersonification, etc.

In the paper by Vijay Kumar et al. [4], the authors propose an efficient user enrollment and user revocation scheme for secure data sharing across the cloud computing environment. Here, the data re-encryption scheme is used, and it aims to effectively address the file

https://doi.org/10.1016/j.compeleceng.2022.107786

Available online 12 February 2022

when it is deleted or updated. The security analysis of this scheme provides better security measures.

In the paper by Gayathri et al. [5], the authors propose a Securely Encrypted Data Access Policies (SEDAP) for cloud computing environments. The objective here is to provide more secure and consistent job administration across the cloud computing environment. The secure hashing algorithm is used for the encryption process.

In the paper by Jegadeesan et al. [6], the authors propose a privacy-preserving scheme for online education systems. This work presents an efficient authentication protocol to resolve the barriers associated with traditional systems. It helps in the management of higher computational cost and offer improved security parameters.

In the paper by Xuyang et al. [7], a privacy-preserving task allocation scheme is proposed for edge computing-assisted mobile crowdsourcing applications. This novel scheme works on the basis of a homomorphic encryption-based algorithm, and it aims to protect the fraudulent activities across the semi-honest edge servers. The effectiveness and availability of this algorithm is found to be comparatively better than conventional approaches.

In the paper by Qazi et al. [8], an intelligent and efficient intrusion detection algorithm based on a a deep learning approach is proposed. The deep learning algorithm is implemented in the tensor flow library and the GPU framework. The accuracy of the work is found to be more than 96%, and it helps in the efficient intrusion classification process.

In the paper by Islam et al. [9], a lattice-based searchable encryption scheme is proposed to secure the Electronic Medical Records (EMR). It provides a lightweight encryption technique with improved security measures. Detailed cryptanalysis of this scheme is made, and it's proven to be more secure than the conventional methods.

In the paper by Sharma et al. [10], the authors propose a blockchain-based approach for securing medical big data in the technological era. It provides efficient security solutions for healthcare applications. This approach transfers the centralized healthcare applications to decentralized systems with no single point of failure. The security and privacy measures of this algorithm are found to be comparatively better than conventional approaches.

3. Final thoughts

We hope this special section will add considerable value to the research community. The guest editor would like to thank all the authors for their valuable contributions and the reviewers for their comments and suggestions. We also would like to take this opportunity to convey our special thanks to the Editor-in-Chief for providing us a privilege to organize this special section, and for his constant support.

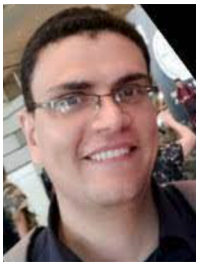
Guest editors:

References

[1] Nguyen, Giang L., et al. "A collaborative approach to early detection of IoT Botnet".
[2] Mohammad, Abdul Salam, and Manas Ranjan Pradhan. "Machine learning with big data analytics for cloud security".
[3] Panda, Suryakanta, Samrat Mondal, and Neeraj Kumar. "SLAP: A Secure and Lightweight Authentication Protocol for machine-to-machine communication in industry 4.0".
[4] Xu, Lu-Jun, et al. "Secure deduplication for big data with efficient dynamic ownership updates".
[5] Nagasubramanian, Gayathri, et al. "Secure and Consistent Job Administration Using Encrypted Data Access Policies in Cloud Systems".
[6] Subramani, Jegadeesan, et al. "Lightweight batch authentication and privacy-preserving scheme for online education system".
[7] Ding, Xuyang, et al. "Privacy-preserving task allocation for edge computing-based mobile crowdsensing".
[8] Emad-ul-Haq Qazi, Muhammad Imran, Noman Haider, Muhammad Shoaib, Imran Razzak, An Intelligent and Efficient Network Intrusion Detection System Using Deep Learning.
[9] Islam, SK Hafizul, et al. "An efficient and forward-secure lattice-based searchable encryption scheme for the Big-data era".
[10] Sharma, Pratima, Malaya Dutta Borah, and Suyel Namasudra. "Improving security of medical big data by using Blockchain technology".

Marimuthu Karuppiah received his Ph.D. degree in Computer Science and Engineering from VIT University, Vellore, India in 2015. Presently, he is a Professor in Department of Computing Science and Engineering, SRM University, Delhi-NCR, India. He has published more than 50 research papers in SCI indexed journals. Also, he has published more than 30 research papers in SCOPUS indexed journals and international conferences. His main research interests include cryptography and wireless network security, in particular, authentication and encryption schemes.

Shehzad Ashraf Chaudhry received Ph.D. degrees (with Distinction) from International Islamic University Islamabad, Pakistan in 2016, respectively. He is currently working as an Associate Professor with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, Istanbul, Turkey. With an H-index of 34, I-10 Index 70 and 108 WoS publications on my credit, my work has been cited more than 1800 times. Considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientist in Pakistan.



Mohammed H. Alsharif received the B.Eng. degree in electrical engineering (communication and control) from the Islamic University of Gaza, Palestine, in 2008, and the M.Sc.Eng. and Ph.D. degrees in electrical engineering (wireless communication and networking) from the National University of Malaysia, Malaysia, in 2012 and 2015, respectively. He joined Sejong University, South Korea, in 2016, where he is currently an Assistant Professor with the Department of Electrical Engineering. His current research interests include wireless communications and networks, including wireless communications, network information theory, IoT, green communication, energy-efficient wireless transmission techniques, wireless power transfer, and wireless energy harvesting.

Marimuthu Karuppiah[a,*], Shehzad Ashraf Chaudhry[b], Mohammed H.M. Alsharif[c]
[a] *SRM Institute of Science and Technology(Deemed to be University), Delhi-NCR Campus, Ghaziabad 201204, India*
[b] *Istanbul Gelisim University, Istanbul, Turkey*
[c] *Sejong University, South Korea*

[*] Corresponding author:
E-mail addresses: marimuthume@gmail.com (M. Karuppiah), ashraf.shehzad.ch@gmail.com (S.A. Chaudhry), malsharif@sejong.ac.kr (M.H.M. Alsharif).