cryptography

MDPI

Editorial

Privacy-Preserving Techniques in Cloud/Fog and Internet of Things

Cheng-Chi Lee [1,2,*], Mehdi Gheisari [3,4], Mohammad Javad Shayegan [5], Milad Taleby Ahvanooey [6,7] and Yang Liu [8]

1 Department of Library and Information Science, Fu Jen Catholic University, New Taipei City 242062, Taiwan
2 Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan
3 Department of Computer Science, Islamic Azad University, Tehran 1468763785, Iran; mehdi.gheisari61@gmail.com
4 Department of Cognitive Computing, Institute of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602105, India
5 Computer Engineering Department, University of Science and Culture, Tehran 1461968151, Iran; shayegan@usc.ac.ir
6 School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798, Singapore; milad.ta@ntu.edu.sg
7 Institute of Computer Science, Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warszawa, Poland
8 Department of Computer Science and Technology, Harbin Institute of Technology, Shenzhen 518055, China; liu.yang@hit.edu.cn
* Correspondence: cclee@mail.fju.edu.tw

1. Introduction

Recently, wireless networks have been developed using cloud infrastructure and software-based networks. Their connections to the next-generation Internet and the Internet of Things (IoT) have reduced costs and improved reliability. It is critical for people, factories, vehicles, road and transportation environments, and much more to use IoT sensors and devices for daily tasks in these vast and complex networks. It is also important to leverage privacy-preservation patterns in large networks such as Big Data and software-based networks. Several supporting technologies for IoT are cloud computing and fog computing. However, the possibility of privacy breaches in these three technologies is high. The main purpose of this Special Issue is to present and compile articles about this topic.

In this Special Issue, we delve into the vanguard of protection—privacy-preserving techniques. From cryptographic algorithms that allow for secure data sharing without compromising privacy to federated learning models that train on decentralized data, our contributors explore the tools and strategies that empower individuals and organizations to regain control over their data.

Our authors elucidate the nuances of preserving privacy in cloud environments, where vast datasets are stored and processed remotely, and fog computing, which extends these capabilities closer to the edge, reducing latency but heightening concerns about data exposure. In the realm of IoT, we confront the challenge of securing devices with limited computational power and the imperative of safeguarding data as they traverse vast networks.

In this Special Issue, we were privileged to receive a total of 21 papers, out of which 10 were selected for publication. The authors have presented a range of innovative ideas and methodologies aimed at addressing the complex issues of security and privacy within cloud/fog and IoT. It is our firm belief that the creation of a secure and highly efficient sensing environment holds the potential to bring immense benefits to people across the globe. We extend our heartfelt gratitude to all the authors for their invaluable contributions to this pivotal field of research.

check for updates

Citation: Lee, C.-C.; Gheisari, M.; Shayegan, M.J.; Ahvanooey, M.T.; Liu, Y. Privacy-Preserving Techniques in Cloud/Fog and Internet of Things. *Cryptography* **2023**, 7, 51. https://doi.org/10.3390/cryptography7040051

Received: 7 October 2023
Accepted: 11 October 2023
Published: 16 October 2023

2. Summary of the Special Issue

In [1], Parrilla et al. proposed a method for area optimization independent of FPGA technology to obtain true random numbers. Most cryptographic algorithms generating a true random number are involved in designing secure cloud/fog and Internet of Things (IoT). They show that their proposed method can pass NIST tests with a low number of ring oscillators and it can be implemented on low-cost FPGAs to produce secure IoT devices. Until now, designing true random number generators for FPGAs is still one of the greatest challenges.

In privacy-preserving techniques, we need a symmetric cryptosystem, such as AES, to encrypt/decrypt communicated messages using a common shared key. In [2], the authors proposed a new shared key generation technique for securing AES. Their research results show that the proposed technique is superior to other existing techniques in terms of security and performance. In addition, the proposed technique successfully passed the key strength analysis tests, such as the frequency test, bit independence test, and bitwise uncorrelation test.

In [3], the authors aimed to explore the problems that password authentication and password polices present within Windows Hello for Business (WHFB). They simulated attacks against user passwords and PINs in WHFB. To solve this issue, one of these solutions is password-less authentication. Two larger organizations such as Microsoft and Google support password-less authentication for end-users and many companies its use for their IT infrastructure. This solution has been tested by millions of people and has been proven to be safe.

In the IoT big data market, some valuable digital assets are growing and accessed in this area. Watermarks are one of the hot topics in the protection of privacy in this market. The authors proposed a blockchain-based resource-efficient anonymity protection with robust watermarking in the IoT big data market [4]. The experimental results showed that the proposed scheme can provide data owners and consumers with ownership and anonymity in view of four different-type IoT datasets: bounded-errors, sub-stream sizes, watermark lengths, and ratios of data tampering. This method can encourage more IoT big data owners, including public sectors, to provide consumers' valuable data with anonymity to further foster more diversified IoT applications.

Information systems' dependability, availability, and cybersecurity are very important security requirements in cloud and IoT systems. To assess these requirements in some relevant indicators, it is necessary to develop and implement tools for Cloud and IoT systems. In [5], the authors proposed a strategy based on the continuous collection, comparison, selection, and combination of Markov and semi-Markov models for assessing these systems. The proposed method was based on the fact that the model design strategy consists of step-by-step selection, adaptation, and possible changes in the type of parameters during the use of the system. This method was found to increase dependability, availability, and cybersecurity assessment trustworthiness.

Smart home IoT is used to connect different home appliances and provide access to them over an insecure network from a remote place. Because of the limited resources of these IoT devices, there is an urgent need for a light weight authentication scheme for smart home IoT devices. The contributions of [6] are as follows. They investigated the most common authentication methods for low-power devices and discovered the drawbacks of the available ones. The authors proposed a generalized authentication method for low-power IoT devices to improve security in remote access scenarios. They analyze the performance of the proposed scheme and showed that it is secure and can prevent many attacks.

In another study, the authors proposed a privacy-preserving federated learning system based on homomorphic encryption for medical data [7]. Due to of the high number of privacy attacks on deep learning models, homomorphic encryption-based model protection from the adversary collaborator was used to solve this problem. The main contributions of [7] are as follows. They provide a practical method to implement secure multi-party

computation in federated learning to improve the privacy and security of medical data, which can protect the confidentiality of the sensitive medical data. A real-world medical dataset was used to evaluate the proposed method and the experimental results showed that the method can protect the deep learning model from adversaries.

The wearable health crowd sensing (WHCS) system enables wearable data collection through active sensing to provide health monitoring to users. Wearable sensing devices can capture data and transmit it to the cloud for data processing and analytics. Due to the bandwidth limitation in WHCS, it is challenging to protect the large data transfers against zero-day attacks. The authors proposed a batch processing scheme for WHCS [8]. The security analysis showed that the proposed scheme is secure against some attacks using the random oracle model. In addition, their performance can achieve lower computation and communication costs with less storage overhead. The results showed that it is superior to other existing batch processing schemes.

Stylometry is a well-known field and uses statistical methods to analyze style in order to determine authorship. It has been applied successfully to several areas such as in historical research or for copyright purposes. However, it may expose users' privacy and personal data in specific contexts without the users being aware of it. The authors of [9] presented the possibility of automated identification of a person using stylometry. They focused and experimented on four types of texts using stylometry: books, articles in blogs, emails, and social media posts. The results showed the effectiveness of stylometry, possible privacy threats, and the relevant legal provisions.

A searchable encryption scheme is used to gain access to a collection of encrypted documents based on a searching functionality using keywords in the documents without the ability to decrypt them. The authors of [10] proposed a searchable encryption system that uses biometric authentication in cloud environments. The proposed system has three components: classical authentication, biometric authentication, and searchable encryption. Through their security and performance analysis, the proposed system was demonstrated to be secure enough for its purposes and efficient for practical implementation. The proposed system will move the Google Cloud Platform and IoT devices in the next direction.

Funding: This research received no external funding.

Acknowledgments: I would like to thank the all authors and anonymous reviewers for their valuable collaboration and contributions to this Special Issue.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Parrilla, L.; García, A.; Castillo, E.; López-Villanueva, J.A.; Meyer-Baese, U. Revisiting Multiple Ring Oscillator-Based True Random Generators to Achieve Compact Implementations on FPGAs for Cryptographic Applications. *Cryptography* **2023**, *7*, 26. [CrossRef]
2. Kulkarni, P.; Khanai, R.; Torse, D.; Iyer, N.; Bindagi, G. Neural Crypto-Coding Based Approach to Enhance the Security of Images over the Untrusted Cloud Environment. *Cryptography* **2023**, *7*, 23. [CrossRef]
3. Haddad, J.; Pitropakis, N.; Chrysoulas, C.; Lemoudden, M.; Buchanan, W.J. Attacking Windows Hello for Business: Is It What We Were Promised? *Cryptography* **2023**, *7*, 9. [CrossRef]
4. Wang, C.-H.; Hsu, C.-H. Blockchain of Resource-Efficient Anonymity Protection with Watermarking for IoT Big Data Market. *Cryptography* **2022**, *6*, 49. [CrossRef]
5. Kharchenko, V.; Ponochovnyi, Y.; Ivanchenko, O.; Fesenko, H.; Illiashenko, O. Combining Markov and Semi-Markov Modelling for Assessing Availability and Cybersecurity of Cloud and IoT Systems. *Cryptography* **2022**, *6*, 44. [CrossRef]
6. Kumar, V.; Malik, N.; Singla, J.; Jhanjhi, N.Z.; Amsaad, F.; Razaque, A. Light Weight Authentication Scheme for Smart Home IoT Devices. *Cryptography* **2022**, *6*, 37. [CrossRef]
7. Wibawa, F.; Catak, F.O.; Sarp, S.; Kuzlu, M. BFV-Based Homomorphic Encryption for Privacy-Preserving CNN Models. *Cryptography* **2022**, *6*, 34. [CrossRef]
8. Addobea, A.A.; Li, Q.; Amankona, I.O.; Hou, J. A Batch Processing Technique for Wearable Health Crowd-Sensing in the Internet of Things. *Cryptography* **2022**, *6*, 33. [CrossRef]

9. Patergianakis, A.; Limniotis, K. Privacy Issues in Stylometric Methods. *Cryptography* **2022**, *6*, 17. [CrossRef]
10. Mihailescu, M.I.; Nita, S.L. A Searchable Encryption Scheme with Biometric Authentication and Authorization for Cloud Environments. *Cryptography* **2022**, *6*, 8. [CrossRef]