applied sciences

MDPI

Editorial

Advances in Information Security and Privacy

Gianluca Lax * and Antonia Russo

Department of Information Engineering, Infrastructure and Sustainable Energy (DIIES), University Mediterranea of Reggio Calabria, 89122 Reggio Calabria, Italy

* Correspondence: lax@unirc.it; Tel.: +39-965-167-3304

1. Introduction

Due to the recent pandemic crisis, many people are spending their days smart working and have increased their use of digital resources for both work and entertainment. This means that the amount of digital information handled online has dramatically increased, and a significant increase in the number of attacks, breaches, and hacks has been observed. This Special Issue aims to establish the state of the art in protecting information by mitigating information risks. This objective is reached by presenting both surveys on specific topics and original approaches and solutions to specific problems. In total, 16 papers have been published in this Special Issue; the following sections provide summaries of these papers grouped by the topics they address.

2. Surveys

Two papers were selected to present an overview of the state of the art in two important topics. Alghofaili Yara et al. [1] present a comprehensive survey regarding security issues at four cloud infrastructure levels: application, network, host, and data. They investigate the most prominent issues that may affect the cloud computing business model with regard to infrastructure and the current solutions used to mitigate different security issues at each of these levels. The second survey published in this Special Issue regards the use of blockchain technology in the development of privacy protocols [2]. This survey classifies the existing solutions based on blockchain fundamental building blocks (smart contracts, cryptography, and hashing) and investigates the evaluation criteria used to validate these techniques. The key factors that strengthen or weaken blockchain privacy are identified, and an evaluation framework to analyze the efficiency of blockchain-based privacy solutions is also formulated.

3. Cryptographic Primitives

Low-level cryptographic algorithms are very important because they are used to build cryptographic protocols for security. In this Special Issue, four papers discuss this topic. Tseng Yi-Fan and Shih-Jie Gao [3] define a new form of inner product encryption to provide fine-grained access control to secure distributed system architectures. The main advantages of this scheme are that it is the first decentralized scheme with constant-size ciphertext and it reduces encryption/decryption costs compared to the state of the art. A new scheme supporting digital signature, encryption, and delegation is proposed in [4]. This scheme requires limited memory space and power; therefore, it has been designed to be used in IoT devices with resource limitations. An important cryptographic primitive is the generation of pseudorandom sequences, because they are especially used in information security. Maksymovych Volodymyr et al. [5] define a new Additive Fibonacci generator scheme in which the introduction of additional structural elements ensures the operation of generators with arbitrary values of the recurrent equation modulus. This innovation improves the statistical characteristics of generators and expands the scope of their use in cryptography, particularly in streaming ciphers. In this section, the proposal presented in [6] is included,

check for updates

Citation: Lax, G.; Russo, A. Advances in Information Security and Privacy. *Appl. Sci.* **2022**, *12*, 7995. https://doi.org/10.3390/app12167995

Received: 8 August 2022
Accepted: 8 August 2022
Published: 10 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

in which a new consensus algorithm is proposed because consensus algorithms are the basis for blockchains. The primary purpose of this algorithm is to improve scalability in terms of validation and verification rates; for this reason, the new algorithm was designed to be used in scenarios in which a limited delay is tolerated. The results of the validation show that the proposed algorithm improves the state of the art in terms of the efficiency of block generation time and transactions per second.

4. Privacy

The topic of privacy has received significant attention in this Special Issue, and four articles discuss this topic. In the field of location-based service, the provision of dummy locations is used to preserve users' privacy. Xu Xianyun, Huifang Chen, and Lei Xie [7] present a dummy location selection algorithm to maximize the anonymous entropy and the effective distance of the candidate location set consisting of the vehicle user's location and dummy locations. This solution ensures the uncertainty and dispersion of selected dummy locations. This proposal is innovative because a trustable third-party server is not needed. Privacy concerns in contact tracing applications are studied in [8], and the conclusion that decentralized solutions are preferable to centralized solutions leads the authors to propose a framework that provides a roadmap on building contact tracing applications within the EU. The framework is validated against common threats and compared with three leading European contact-tracing implementations. The possibility that a firm is involved in privacy infringement cases resulting in legal causations is studied in [9]. This study exploits machine learning and text analysis to build a model that can predict legal judgment using information related to societal factors and technological development. Tor is the most popular anonymous communication protocol used to protect the personal privacy of its users. The study presented in [10] highlights that anonymity is broken if an adversary can monitor the traffic at the bounds of the Tor circuit. Thus, the authors propose an improvement of the protocol based on probabilistic encryption to effectively protect users' privacy.

5. Authentication

In the field of the Internet of Vehicles, achieving both the privacy and traceability of nodes is a challenging task. To address this need, Qureshi Kashif Naseer et al. [11] present an authentication scheme based on blockchain to provide vehicle nodes with mechanisms to become anonymous and take control of their data during the data communication process. The proposed scheme has been implemented by utilizing Hyperledger Fabric as a blockchain and provides conditional privacy to users and vehicles to ensure the anonymity, traceability, and unlinkability of data sharing among vehicles. Passwords are the most commonly used mechanism for authentication, and the use of password checkers to prevent users from creating easy-to-guess passwords is considered the best practice. The study presented in [12] analyzes how Markov models can help create a more effective password checker that would be able to check the probability of a given password to be chosen by an attacker. The authors determine that one Markov model is insufficient for the creation of a more effective password checker, and multiple Markov models are required to carry out strength calculations for a wide range of passwords.

6. Database Security

The obtainment of convincing evidence of database security and the quantification of a measure of database security is an important topic. Yesin Vitalii et al. [13] present a technique for the evaluation of the security of relational databases based on the enhanced theoretical Clements–Hoffman model. The degree of security is calculated on the basis of an integral quantitative metric that is the reciprocal of the total residual risk associated with the possibility of implementing threats in relation to a database object when using security measures. The main techniques implemented in accordance with the recommendations of the Clark–Wilson model to ensure the integrity of data and persistent stored database modules are studied in [14]. The authors propose a mechanism to ensure the integrity of the data and programs of databases based on the provisions of the relational database theory, the Row Level Security technology, the potential of the modern blockchain model, and the capabilities of the database management system on the platform of which databases with the universal basis of relations are implemented. By applying this mechanism, it is guaranteed that the stored data and programs remain correct, unaltered, undistorted, and preserved.

7. Regulation

The General Data Protection Regulation (GDPR) is the most important regulation regarding data protection and privacy in the European Union. Ensuring the reliability and integrity of the personal data processing request records of a data subject to enable its utilization according to the GDPR requirements is the challenge investigated in [15]. In this paper, the authors propose a notarization framework using a private blockchain to allow the data subject to delegate requests to process personal data. In this framework, the requests are handled by a data controller, and the generated data request and processing result data are stored in the blockchain ledger and notarized via a trusted institution of the blockchain network. This framework has been implemented with Hyperledger Fabric to demonstrate the fulfillment of system requirements and the feasibility of implementing a GDPR compliance audit for the processing of personal data. A comparison of the legislation on data protection topics in the various EU member states is studied in [16]. The study is limited to 19 states whose national supervisory authorities agreed to participate in the research by answering a prepared survey about data protection issues. Among many other findings, an interesting result is that in most of the cases, member states do not have any additional/specific legislation on data protection.

Acknowledgments: This issue would not have been possible without the contributions of the authors, reviewers, and the editorial team of *Applied Sciences*. Congratulations to all authors; we are sure that their research will receive many downloads and citations in the coming years. We would like to thank the editorial team of *Applied Sciences* for always being present during the whole process of the creation of this Special Issue.

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

References

1. Alghofaili, Y.; Albattah, A.; Alrajeh, N.; Rassam, M.; Al-rimy, B. Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. *Appl. Sci.* **2021**, *11*, 9005. [CrossRef]
2. Junejo, A.; Hashmani, M.; Memon, M. Empirical Evaluation of Privacy Efficiency in Blockchain Networks: Review and Open Challenges. *Appl. Sci.* **2021**, *11*, 7013. [CrossRef]
3. Tseng, Y.; Gao, S. Decentralized Inner-Product Encryption with Constant-Size Ciphertext. *Appl. Sci.* **2022**, *12*, 636. [CrossRef]
4. Chen, M.; Huang, H. A Practical and Efficient Node Blind SignCryption Scheme for the IoT Device Network. *Appl. Sci.* **2022**, *12*, 278. [CrossRef]
5. Maksymovych, V.; Shabatura, M.; Harasymchuk, O.; Karpinski, M.; Jancarczyk, D.; Sawicki, P. Development of Additive Fibonacci Generators with Improved Characteristics for Cybersecurity Needs. *Appl. Sci.* **2022**, *12*, 1519. [CrossRef]
6. Uddin, M.; Muzammal, M.; Hameed, M.; Javed, I.; Alamri, B.; Crespi, N. CBCIoT: A Consensus Algorithm for Blockchain-Based IoT Applications. *Appl. Sci.* **2021**, *11*, 11011. [CrossRef]
7. Xu, X.; Chen, H.; Xie, L. A Location Privacy Preservation Method Based on Dummy Locations in Internet of Vehicles. *Appl. Sci.* **2021**, *11*, 4594. [CrossRef]
8. Storm van Leeuwen, D.; Ahmed, A.; Watterson, C.; Baghaei, N. Contact Tracing: Ensuring Privacy and Security. *Appl. Sci.* **2021**, *11*, 9977. [CrossRef]
9. Park, M.; Chai, S. AI Model for Predicting Legal Judgments to Improve Accuracy and Explainability of Online Privacy Invasion Cases. *Appl. Sci.* **2021**, *11*, 11080. [CrossRef]
10. Buccafurri, F.; De Angelis, V.; Idone, M.; Labrini, C.; Lazzaro, S. Achieving Sender Anonymity in Tor against the Global Passive Adversary. *Appl. Sci.* **2022**, *12*, 137. [CrossRef]
11. Qureshi, K.; Shahzad, L.; Abdelmaboud, A.; Elfadil Eisa, T.; Alamri, B.; Javed, I.; Al-Dhaqm, A.; Crespi, N. A Blockchain-Based Efficient, Secure and Anonymous Conditional Privacy-Preserving and Authentication Scheme for the Internet of Vehicles. *Appl. Sci.* **2022**, *12*, 476. [CrossRef]

12. Taneski, V.; Kompara, M.; Heričko, M.; Brumen, B. Strength Analysis of Real-Life Passwords Using Markov Models. *Appl. Sci.* **2021**, *11*, 9406. [CrossRef]
13. Yesin, V.; Karpinski, M.; Yesina, M.; Vilihura, V.; Rajba, S. Technique for Evaluating the Security of Relational Databases Based on the Enhanced Clements-Hoffman Model. *Appl. Sci.* **2021**, *11*, 11175. [CrossRef]
14. Yesin, V.; Karpinski, M.; Yesina, M.; Vilihura, V.; Warwas, K. Ensuring Data Integrity in Databases with the Universal Basis of Relations. *Appl. Sci.* **2021**, *11*, 8781. [CrossRef]
15. Jung, S.; Lee, S.; Euom, I. Delegation-Based Personal Data Processing Request Notarization Framework for GDPR Based on Private Blockchain. *Appl. Sci.* **2021**, *11*, 10574. [CrossRef]
16. Hölbl, M.; Kežmah, B.; Kompara, M. Data Protection Heterogeneity in the European Union. *Appl. Sci.* **2021**, *11*, 10912. [CrossRef]