applied sciences

MDPI

Editorial

Advanced Technologies in Data and Information Security

George Drosatos [1,*], Konstantinos Rantos [2] and Konstantinos Demertzis [3]

[1] Institute for Language and Speech Processing, Athena Research Center, 67100 Xanthi, Greece
[2] Department of Computer Science, International Hellenic University, 65404 Kavala, Greece; krantos@cs.ihu.gr
[3] Department of Physics, International Hellenic University, 65404 Kavala, Greece; kdemertzis@teiemt.gr
* Correspondence: gdrosato@athenarc.gr; Tel.: +30-25410-78787 (ext. 322)

1. Introduction

The protection of personal data and privacy is a timeless challenge which has intensified in the modern era. The digitisation that has been achieved in recent decades has radically changed the way we live, communicate and work, revealing various security and privacy issues. Specifically, the explosion of new technologies and the continuous developments of technologies, such as the Internet of Things (IoT) and Artificial Intelligence (AI), have led to the increased value of data, while it has raised demand and introduced new ways to obtain it. Techniques such as data analysis and processing provide a set of powerful tools that can be used by both governments and businesses for specific purposes. However, as with any valuable resource, as in the case of data, the phenomena of abuse, unfair practices and even criminal acts are not absent. In particular, in recent years, there have been more and more cases of sophisticated cyberattacks, data theft and leaks or even data trade, which violate the rights of individuals, but also harm competition and seriously damage the reputation of businesses.

With this in mind, the present Special Issue of *Applied Sciences* on "*Advanced Technologies in Data and Information Security*" provides an overview of the latest developments in this field. Nineteen papers were submitted to this Special Issue, and nine papers [1–9] were accepted (i.e., an 47.4% acceptance rate). The presented papers explore innovative trends of data privacy and information security that enable technological breakthroughs in high-impact areas and cover several topics, mainly regarding blockchain technology, secure multi-party computation, threat detection, trusted execution environment, as well as cyberawareness, security level estimation and security policy compliance.

2. Blockchain Technology

Blockchain technology is one of the latest security technologies that has attracted the increasing attention of various actors in many fields, including the educational sector and the Internet of Vehicles.

Ayub Khan et al. [1] proposed HEDU-ledger, a secure architecture for attestation, verification and traceability of higher education degrees based on a private permissioned blockchain network, and in particular the Hyperledger Fabric. The HEDU-Ledger architecture is a complete decentralised solution that first endorses attestation records, and then validates the degree and maintains the secure chain between the stakeholder peer nodes. The stakeholders and other connecting parties are initially identified and authenticated by the Higher Education Commission (HEC) using digital signatures. Moreover, the authors presented the entire mechanism of the proposed architecture, including the HEC policy, the attestation and verification criteria, and the other elements involved in the procedures. Finally, HEDU-Ledger also records more details about the stored ledger in an IPFS (InterPlanetary File System) data storage structure in protected and immutable form.

Delgado-von-Eitzen et al. [2] conducted a systematic literature review providing an overview of the current state-of-the-art related to blockchain applications in education.

check for updates

Citation: Drosatos, G.; Rantos, K.; Demertzis, K. Advanced Technologies in Data and Information Security. *Appl. Sci.* **2022**, *12*, 5925. https://doi.org/10.3390/app12125925

Received: 19 May 2022
Accepted: 9 June 2022
Published: 10 June 2022

The systematic review was based only on articles published in peer-reviewed journals, that were identified by searching eleven scientific databases. The analysed papers answered research questions about the current state of blockchain applications in education, the features of blockchain that could benefit this sector, and the challenges that need to be addressed. According to the authors' findings, there are no widely used blockchain solutions in education, but only models, pilots and proofs of concept. However, the progress is continuous and the initiatives are becoming more and more interesting, as they prove that blockchain can be a key technology in future educational scenarios.

In another direction, Kaltakis et al. [3] performed a literature review to identify proposed solutions for different sectors of Internet of Vehicles (IoV), which use blockchain technology, while also attempting to protect the privacy of involved parties. The privacy protection concerns users' identity, vehicles' location and exchange data between vehicles and infrastructures. In this context, the authors analysed the main characteristics and properties of existing solutions to provide a comprehensive and critical overview and identified their contribution to the field. Moreover, this review provides researchers with suggestions for future work in the field of privacy-preserving blockchain-enabled solutions for vehicular networks.

3. Secure Multi-Party Computation

With the development of privacy-enhancing technologies, the growing demand for performing secure multi-party computations (MPC) on mobile devices has become a major challenge. In this direction, Tang et al. [4] proposed an efficient two-party computation protocol, called LPCP (Lightning Polynomial Computation Protocol), which is secure against semi-honest adversaries and is based on the Chinese Remainder Theorem (CRT). The proposed privacy-preserving protocol utilises CRT-based encryption and re-encryption techniques to perform additive and multiplicative homomorphic encryption, which can be transformed into a secure two-party polynomial calculation scheme. In addition, the authors presented an extension of the two-party LPCP protocol to a multi-party LPCP protocol, which is faster and less space-intensive than other existing approaches. As a proof-of-concept, based on LPCP, a distance measurement computation protocol was introduced, which shows that it is affordable for mobile devices. The experimental evaluation of the proposed LPCP scheme in ARM and x86 architecture environments showed that it has a great advantage of both execution time and communication overhead, compared to the state-of-the-art two-party and multi-party computation protocols, allowing the implementation of secure calculations on mobile devices.

4. Threat Detection

Nowadays, the detection and classification of threats is one of the most important problems in cybersecurity, as the new tactics employed by adversaries have become even more sophisticated and advanced. A solution in this direction is the one presented by Pérez-Sánchez and Palacios [5]. More precisely, they proposed a threat detection strategy based on the analysis of events generated by the system and the corresponding mapping of the risk level with the MITRE ATT&CK matrix and the Cyber Kill Chain. The proposed event-based analysis method could stop the attack at the right moment, when it reaches the "Execution/Exploitation" state, preventing any `PowerShell` or `Cmd` calls. The validation of the aforementioned detection strategy was performed experimentally using a comparative study against 10 traditional antivirus detection systems, always using the same set of samples and with the same obfuscation technique applied to the malware code in each case. The results showed that the proposed methodology was able to detect threats even if obfuscation techniques were applied, which was not the case with all antivirus software.

5. Trusted Execution Environment

A recent innovation in hardware-level security is the technologies of Trusted Execution Environment (TEE). In the paper published by Kim [6], an application-level optimisation

methodology was proposed using asynchronous switchless calls to reduce SGX overhead. Intel Software Guard Extensions (SGX) is an extension of x86 instruction set architecture that provides hardware-protected isolation, suitable for privacy-preserving computations. Accordingly, the switchless call operates enclave entries and exits asynchronously with worker threads to reduce enclave transition, similar to asynchronous I/O implementation in operating systems. More precisely, the author developed a heuristic method for deriving a metric, switchless efficiency, based on a comprehensive analysis of switchless calls. To demonstrate that the proposed methodology meets the design goal, a case study was conducted optimising a performance-critical network application, an SGX-enabled network middlebox. The evaluation showed that the proposed optimisation successfully improves the performance of the SGX-enabled middlebox, while a naive adoption of switchless calls degrades its performance.

6. Cyberawareness, Security Level Estimation and Security Policy Compliance

The daily digital exposure to the Internet, the increasing digitalisation of Internet services, and the misbehaviour of employees regarding information security have increased the need for better cybernetic awareness, the assessment of security level in online services, and compliance with security policies.

Antunes et al. [7] described a three-fold integrated cybersecurity and cyberawareness strategy for schools, consisting of an assessment of risky attitudes and behaviours in cybersecurity, a self-diagnosis web application to measure students' cybersecurity skills, and a cyberawareness lesson plan. This strategy was implemented and tested in a junior high school, with sixth- and ninth-grade students. The assessment of risky attitudes and behaviours was achieved with the development of two new questionnaires, namely, Cybersecurity Behaviours in Schools (CsB-S), and Cybersecurity Attitudes in Schools (CsA-S). Both questionnaires were completed by 164 students, the web self-diagnosis application became available to the same students who also benefited from the implementation of a lesson plan designed for digital citizenship courses. Regarding the results that emerged from the assessment of attitudes and behaviours, although positive, the authors observed that the attitudes and behaviours in ninth-grade students are globally inferior compared to those attained by sixth-grade students. Although the proposed cyberawareness strategy was applied in a school context, the authors noted that it can be applied in other contexts as well, such as enterprises, healthcare institutions and the public sector.

Ramanauskaitė et al. [8] proposed a security level estimation model for educational organisations, without requiring the usage of external security experts. This model takes into account the specifics of distance learning and allows the quantitative estimation of an organisation's security level. To achieve this, it relies on values of 49 quantitative criteria, structured into an Analytic Hierarchy Process (AHP) tree, and arranged to the final estimation score of security level by incorporating criteria of importance based on the opinion of experts. The validation of the proposed model confirmed that the model meets the expert-based security ranking and can be used as a simpler alternative security model in educational organisations.

Finally, Ali et al. [9] conducted a systematic literature review over the last decade (2010–2020), highlighting the Information Security Behaviour (ISB), its factors, and its theoretical implications for Information Security Policy Compliance (ISPC). More precisely, the main focus was to determine the transformation of behaviour from non-compliance to compliance behaviour. For this reason, the researchers reviewed the literature in two dimensions: (1) studies measuring compliance behaviour; (2) studies measuring non-compliance behaviour. The findings showed that ISPC research focused more on compliance than non-compliance behaviours. Regarding non-compliance, many factors play a role, such as value conflicts, security-related stress, and neutralisation. On the other hand, internal, external and protection motivations in an organisation proved to be positively important in terms of compliance behaviours. Deterrence techniques, management behaviours, culture, and information security awareness play a vital role in transforming employees'

non-compliance into compliance behaviours. Overall, this systematic review contributes to information system security literature by providing a behaviour transformation process model based on the existing ISPC literature.

Author Contributions: Conceptualization, G.D., K.R. and K.D.; writing—original draft preparation, G.D.; writing—review and editing, K.R. and K.D.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Ayub Khan, A.; Laghari, A.A.; Shaikh, A.A.; Bourouis, S.; Mamlouk, A.M.; Alshazly, H. Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission. *Appl. Sci.* **2021**, *11*, 917. [CrossRef]
2. Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. Blockchain Applications in Education: A Systematic Literature Review. *Appl. Sci.* **2021**, *11*, 1811. [CrossRef]
3. Kaltakis, K.; Polyzi, P.; Drosatos, G.; Rantos, K. Privacy-Preserving Solutions in Blockchain-Enabled Internet of Vehicles. *Appl. Sci.* **2021**, *11*, 9792. [CrossRef]
4. Tang, J.; Cao, Z.; Shen, J.; Dong, X. LPCP: An efficient Privacy-Preserving Protocol for Polynomial Calculation Based on CRT. *Appl. Sci.* **2022**, *12*, 3117. [CrossRef]
5. Pérez-Sánchez, A.; Palacios, R. Evaluation of Local Security Event Management System vs. Standard Antivirus Software. *Appl. Sci.* **2022**, *12*, 1076. [CrossRef]
6. Kim, S. An Optimization Methodology for Adapting Legacy SGX Applications to Use Switchless Calls. *Appl. Sci.* **2021**, *11*, 8379. [CrossRef]
7. Antunes, M.; Silva, C.; Marques, F. An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context. *Appl. Sci.* **2021**, *11*, 1269. [CrossRef]
8. Ramanauskaitė, S.; Urbonaitė, N.; Grigaliūnas, Š.; Preidys, S.; Trinkūnas, V.; Venčkauskas, A. Educational Organization's Security Level Estimation Model. *Appl. Sci.* **2021**, *11*, 8061. [CrossRef]
9. Ali, R.F.; Dominic, P.D.D.; Ali, S.E.A.; Rehman, M.; Sohail, A. Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Appl. Sci.* **2021**, *11*, 3383. [CrossRef]