electronics

MDPI

Editorial

Recent Advances in Information Security and Data Privacy

Jianhua Yang [1,*], Lixin Wang [1], Linqiang Ge [1] and Radhouane Chouchane [2]

[1] TSYS School of Computer Science, Columbus State University, Columbus, GA 31907, USA; wang_lixin@columbusstate.edu (L.W.)
[2] Computer Science Department, Morgan State University, Baltimore, MD 21251, USA
* Correspondence: yang_jianhua@columbusstate.edu

1. Introduction and Recent Developments

The rapid growth of data-driven computing systems—including Internet of Things (IoT) infrastructures, cloud computing platforms, edge computing, mobile/embedded devices, and Artificial Intelligence (AI)-enabled services—has ushered in unprecedented computational efficiency while simultaneously introducing severe vulnerabilities. Safeguarding information security, data privacy, confidentiality, integrity, and authenticity in these highly distributed, often untrusted computing environments is more critical than ever.

Contemporary information security research occupies a unique intersection of computer science, cryptography, legal scholarship, behavioral economics, and policy analysis. Challenges that were once considered largely technical in nature—such as the design of secure communication protocols or the detection of malicious network traffic—have become inextricably intertwined with questions of governance, human rights, and organizational resilience. The advent of machine learning and Artificial Intelligence has simultaneously introduced powerful new defensive capabilities and novel attack vectors, compelling the research community to continually reassess foundational assumptions about trust, identity, and system integrity.

Data privacy, though conceptually distinct from information security, has increasingly converged with it in both research and practice. The enforcement of comprehensive regulatory frameworks—most notably the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and a growing body of analogous national legislation—elevated privacy from a supplementary engineering concern to a primary design objective. Organizations must now navigate complex obligations regarding data minimization, purpose limitation, consent management, and cross-border data transfer, often in the absence of clear technical standards or precedent.

It is against this backdrop that the present Special Issue was conceived. Recognizing the need for a focused, interdisciplinary forum in which cutting-edge theoretical contributions and rigorous empirical findings could be brought into productive dialog, the editorial board invited submissions addressing the most pressing advances and open problems in information security and data privacy. The response from the research community was both substantial and diverse, reflecting the breadth and vitality of the field. This Special Issue, "Recent Advances in Information Security and Data Privacy," including 11 research papers, addresses the critical need for resilient, privacy-preserving data and information systems and aims to highlight the cutting-edge research, theoretical developments, and practical implementations addressing the latest challenges in information security and data privacy.

Check for updates

Received: 22 May 2026
Accepted: 6 June 2026
Published: 22 June 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

2. Overview of the Contributions

The issue opens with a quantum-enabled data authentication without classical control interaction. The authors presented a quantum-assisted data authentication protocol that integrates classical information-theoretic security with quantum communication techniques. It is assumed that only the participants have access to open classical and quantum channels and share a random static key material. Building on the Wegman–Carter paradigm, their scheme employs universal hashing for message authentication and leverages quantum channels to securely transmit random nonces, eliminating the need for key recycling. The protocol utilizes polar codes within Wyner's wiretap channel model to ensure confidentiality and reliability, even in the presence of an all-powerful adversary. Security analysis demonstrates that the protocol inherits strong guarantees from both classical and quantum frameworks and provides the quantum channel maintaining low loss and noise.

New approaches to detect intrusion were explored by two papers. One focused on a neural network and the other focused on modeling and utilizing network traffic to detect stepping-stone intrusion. The study evaluated the robustness of a *Random Forest (RF)*, a standard *neural network (NN)*, and a Transformer-based *Network Intrusion Detection System (NIDS)*. The authors also introduced *ADV_NN*, an adversarial trained neural network designed to improve resilience. Model performance was tested using the UNSW-NB15 dataset under both clean and adversarial conditions. The proposed *ADV_NN* achieved 86.04% accuracy on clean data. It maintained over 80% accuracy under *PGD* and *FGSM* attacks and exceeded 85% under *Black-Box* attacks, while *RF*, *NN*, and Transformer-based models suffered from significant degradation under adversarial perturbations. Stepping-stone intrusion has become a professional and primary way used by intruders to launch their attacks since they can be protected behind a long TCP connection chain. Most algorithms proposed cannot resist intruders' session manipulation. In this issue, the researchers propose a novel approach using the distribution of round-trip time (RTT) of network traffic to detect stepping-stone intrusion. The approach can resist intruders' chaff perturbation since the round-trip time of network packets can fairly be affected by chaffed packets. The experimental results showed that stepping-stone intrusion can be effectively detected and session manipulation can be resisted completely by modeling and utilizing network traffic distribution.

Some hot topics are also involved in this Special Issue, including the CPace protocol, a Proof-of-Friendship Consensus mechanism for resilient blockchain, a scalable and area-efficient accelerator designed to support multiple PQC schemes, and HAETAE on ARMv8. The CPace protocol is a password-authenticated key exchange optimized for simplicity. It involves only two messages exchanged in an arbitrary order and combines a simple and elegant design with privacy guarantees obtained via strict mathematical proofs. Traditional blockchain consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), face significant challenges related to the centralization of validators and miners, environmental impact, and trustworthiness. They not only lack fairness and sustainability but also fail to address social trust dynamics within validator selection. To bridge this research gap, the researchers propose Proof of Friendship (PoF)—a novel consensus mechanism that leverages social trust by improving decentralization, enhancing fairness and sustainability among the validators. The Post-Quantum Cryptosystem (PQC) scheme is supported by a scalable and area-efficient hardware accelerator. With the specially designed accelerator, it can achieve an area efficiency of up to 81.85% compared to the current state-of-the-art multi-scheme accelerator. It addresses the quantum computing threat to cryptography security. In the research of HATETAE on ARMv8, the authors presented a highly optimized implementation of the HAETAE algorithm. To the best of our knowledge,

this is the first optimized implementation of the HAETAE algorithm on 64-bit ARMv8 embedded processors.

Two papers focused on data-hiding techniques in different contexts. Data hiding in digital images is an important cover communication technique. Using adaptive prediction difference coding can achieve lossless data hiding in VQ (vector quantization) compressed images. This technique is implemented through a modified adaptive index rearrangement (AIR) to rearrange a codebook, and, thus, to enhance the correlation of the adjacent indices in the index tables of cover images. The experimental results demonstrate that the proposed scheme can reduce the pure compression rate compared with the existing state-of-the-art algorithms. Reversible data hiding can be applied to crypto-space images with polynomial secret sharing over a Galois Field. Secret sharing is a data security technique that divides secret information into multiple parts, embeds these parts into various shares, and distributes these shares to different participants. The proposed method enables the independent extraction of images and data, ensuring that the recovered images and extracted data can serve as validation information for each other. The method not only enhances data security but also guarantees the accuracy of the extracted information.

A complementary contribution examines the privacy essentials and an evaluation framework for cybersecurity maturity aligned with the NIST CSF. The governance dimension of data privacy is addressed by a rigorous legal–technical analysis of consent management platforms and their capacity to satisfy the substantive requirements of the UK GDPR's transparency and freely given consent provisions. Drawing on both doctrinal legal analysis and a large-scale empirical audit of deployed platforms, the authors reveal the systematic deficiencies in current commercial implementations and propose a principled design framework reconciling user autonomy, usability, and regulatory compliance. This contribution exemplifies the productive synthesis of legal and technical expertise that characterizes the most impactful contemporary privacy scholarship. Cybersecurity is critical for mitigating the economic and reputational impacts of cyberattacks. To address these risks, frameworks like the NIST Cybersecurity Framework (NIST CSF) provide standardized guidelines for managing and reducing cybersecurity threats. A maturity assessment approach aligned with the NIST CSF, incorporating a dual-survey methodology, is presented in this Special Issue.

3. Future Research Directions

Several recurrent themes emerge from a reading of the contributions assembled in this issue that merit particular attention from the research community. First, the tension between utility and privacy—manifest in the federated learning, genomic data sharing, and consent management contributions alike—remains one of the most fundamental and least resolved problems in the field. While techniques such as differential privacy, secure multiparty computation, and homomorphic encryption offer promising avenues, significant challenges remain in terms of scalability, usability, and the precise quantification of privacy loss under composition.

Second, the increasing deployment of AI and machine learning in security-critical contexts introduces a class of systemic risks that existing threat models are not well-equipped to capture. The opacity of large neural networks, their susceptibility to adversarial perturbation, and the potential for unintended information leakage through model outputs collectively constitute a research agenda of considerable urgency. The contributions in this issue represent meaningful progress, but much remains to be done before robust, formally verifiable security guarantees can be extended to AI-augmented systems.

Third, the regulatory landscape continues to evolve at a pace that frequently outstrips both technical capability and scholarly understanding. The coming years will likely witness

the proliferation of AI-specific data protection obligations, mandatory algorithmic auditing requirements, and increased international divergence in privacy norms. Research that bridges normative legal analysis and rigorous technical assessment will be essential to inform both regulatory design and organizational compliance strategy.

Finally, the human and organizational dimensions of information security and data privacy deserve greater attention than they have historically received in technically oriented publication venues. Social engineering remains among the most potent attack vectors available to adversaries; privacy attitudes and behaviors are shaped by cultural, psychological, and socioeconomic factors that resist purely technical remediation; and the effectiveness of even technically sound security controls depends heavily upon the organizational contexts in which they are deployed. We encourage future submissions to the Recent Advances in Information Security and Data Privacy, 2nd Edition, that engage seriously with these dimensions.

4. Acknowledgments

The guest editors wish to express their sincere gratitude to the Editor-in-Chief and the editorial board of the journal for their support of this Special Issue "Recent Advances in Information Security and Data Privacy". We are deeply indebted to the contributing authors for the quality and originality of their work, and to the reviewers whose meticulous and constructive engagement with the submissions was indispensable to the integrity of the selection process. The quality of peer review is the quiet infrastructure of research, rarely celebrated and easily taken for granted. Their diligence, expertise, and willingness to engage critically with the work of their peers have made the Special Issue a stronger collection than it would otherwise have been.

The challenges of information security and data privacy will not be resolved by any single issue of any journal. But the research gathered here advances the conversation in meaningful ways—deepening our understanding of specific vulnerabilities, proposing novel defensive mechanisms, and, perhaps most valuably, asking harder questions about what information security and data privacy are ultimately for. We hope that the present collection serves as both a useful reference for established researchers and an accessible point of entry for those newly entering this vital and rapidly evolving field.

Author Contributions: Writing-original draft preparation, J.Y.; review and editing, L.W., L.G. and R.C. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement: No new data were created.

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

List of Contributions

1. Taylor, J.; Henriksen-Bulmer, J.; Yucel, C. Privacy Essentials. *Electronics* **2024**, *13*, 2263. https://doi.org/10.3390/electronics13122263.
2. Lu, H.; Liu, J.; Chang, C.; Horng, J. Reversible Data Hiding in Crypto-Space Images with Polynomial Secret Sharing over Galois Field. *Electronics* **2024**, *13*, 2860. https://doi.org/10.3390/electronics13142860.
3. Yang, J.; Wang, L. Explore Utilizing Network Traffic Distribution to Detect Stepping-Stone Intrusion. *Electronics* **2024**, *13*, 3258. https://doi.org/10.3390/electronics13163258.
4. Jung, H.; Oh, H. Designing a Scalable and Area-Efficient Hardware Accelerator Supporting Multiple PQC Schemes. *Electronics* **2024**, *13*, 3360. https://doi.org/10.3390/electronics13173360.
5. Chen, S.; Liu, J.; Chang, C.; Chang, C. Lossless Data Hiding in VQ Compressed Images Using Adaptive Prediction Difference Coding. *Electronics* **2024**, *13*, 3532. https://doi.org/10.3390/electronics13173532.
6. Sim, M.; Lee, M.; Seo, H. HAETAE on ARMv8. *Electronics* **2024**, *13*, 3863. https://doi.org/10.3390/electronics13193863.

7. Marchang, J.; Srikanth, R.; Keishing, S.; Kashyap, I. Proof-of-Friendship Consensus Mechanism for Resilient Blockchain Technology. *Electronics* **2025**, *14*, 1153. https://doi.org/10.3390/electronics14061153.
8. Bernardo, L.; Malta, S.; Magalhães, J. An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. *Electronics* **2025**, *14*, 1364. https://doi.org/10.3390/electronics14071364.
9. Heydari, V.; Nyarko, K. Enhancing Adversarial Robustness in Network Intrusion Detection: A Novel Adversarially Trained Neural Network Approach. *Electronics* **2025**, *14*, 3249. https://doi.org/10.3390/electronics14163249.
10. Kutyłowski, M.; Kubiak, P.; Kostkiewicz, P. CPace Protocol—From the Perspective of Malicious Cryptography. *Electronics* **2025**, *14*, 3382. https://doi.org/10.3390/electronics14173382.
11. Zawadzki, P.; Dziwoki, G.; Kucharczyk, M.; Machniewski, J.; Sułek, W.; Izydorczyk, J.; Izydorczyk, W.; Kłosowski, P.; Dustor, A.; Filipowski, W.; et al. Quantum Enabled Data Authentication Without Classical Control Interaction. *Electronics* **2025**, *14*, 4037. https://doi.org/10.3390/electronics14204037.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.