

Advances and Future Directions in Information Security and Data Privacy

Mina Alishahi

Department of Computer Science, Open University, 6401 DL Heerlen, The Netherlands;
mina.sheikhalishahi@ou.nl

1. Introduction

In the last decade, information security and data privacy have emerged as defining concerns in the digital era, shaping technological innovation, policy discourse, and societal trust [1–4]. The increasing integration of networked systems into everyday life—from embedded devices in critical infrastructures to ubiquitous Internet of Things (IoT) applications—has led to unprecedented volumes of sensitive data being collected, processed, and transmitted [2,5–8]. While advances in cryptography, secure architectures, and privacy-preserving algorithms have brought substantial progress, the sophistication of adversarial attacks, the complexity of multi-layered systems, and the rise of AI-driven applications continue to challenge conventional approaches to security [2,5,6,9–12].

The research community has responded with a wide array of methods, spanning from low-level physical-layer protections to high-level policy and governance frameworks [7,11,13,14]. Yet, important questions remain: How can privacy be preserved without degrading functionality? How can systems be secured in environments with imperfect information or untrusted intermediaries? How should emerging AI technologies be integrated responsibly without exacerbating security vulnerabilities?

This Special Issue, *Information Security and Data Privacy*, captures these questions at a moment of rapid change. Across eight contributions—spanning embedded systems, IoT, AI-based privacy methods, federated learning, anonymization, wireless channel security, and next-generation architectures—the collection reflects both the maturity and the evolving frontiers of the field. The works presented here are united by a commitment to tackling real-world security and privacy challenges through rigorous, innovative, and often interdisciplinary approaches.



Received: 9 September 2025
Accepted: 23 September 2025
Published: 26 September 2025

Citation: Alishahi, M. Advances and Future Directions in Information Security and Data Privacy. *Entropy* **2025**, *27*, 1004. <https://doi.org/10.3390/e27101004>

Copyright: © 2025 by the author. 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 (<https://creativecommons.org/licenses/by/4.0/>).

2. Overview of Published Articles

Two contributions address the reliability and integrity of software systems in mission-critical and resource-constrained environments. Zhao et al. (Contribution 1) present *ESfix*, an embedded program repair tool designed to effectively eliminate concurrency defects, with applications in aerospace, medical devices, and other domains requiring high assurance. Wu et al. (Contribution 3) propose a multi-factor authentication-based remote data backup scheme that strengthens security against data loss and tampering, even in untrusted backup environments.

Privacy and security in the IoT domain are tackled by Zhai et al. (Contribution 2), who develop a coercion-resistant attribute-based encryption scheme with policy revocation—an important step toward protecting sensitive data in large-scale IoT ecosystems. At the physical layer, Ta et al. (Contribution 7) introduce a novel noise injection strategy that

guarantees zero secrecy outage probability under imperfect channel state information, offering robust protection in wireless communication scenarios.

The intersection of AI and privacy is represented in three works. You et al. (Contribution 4) leverage diffusion models to generate face privacy-protected images with high visual quality, addressing shortcomings of existing obfuscation methods. Li et al. (Contribution 5) propose LF3PFL, a local federalization-based federated learning framework that enhances privacy without sacrificing model performance. Khatir et al. (Contribution 6) present a greedy, information-theoretic clustering algorithm for anonymizing microdata, balancing privacy with data utility in k-anonymity contexts.

Finally, Kang et al. (Contribution 8) provides a broad perspective with a comprehensive survey on zero trust security, synthesizing theoretical foundations, implementation strategies, and the paradigm's implications for future cybersecurity architectures.

3. Conclusions and Future Directions

Taken together, these contributions advance the state of the art in multiple dimensions: securing embedded systems, safeguarding IoT communications, fortifying wireless channels, anonymizing data, and enhancing privacy in AI-driven and collaborative learning environments. The diversity of methods—ranging from algorithmic innovations to architectural paradigms—underscores the multifaceted nature of modern security challenges.

Looking forward, the field will benefit from:

- **Integrated approaches** that combine complementary techniques, such as merging zero trust principles with privacy-preserving machine learning.
- **Scalable, adaptive defenses** capable of responding in real time to evolving threats, especially in IoT and federated environments.
- **Human-centered security** that accounts for usability, policy, and governance alongside technical robustness.
- **Bridging theory and practice**, ensuring that cutting-edge methods can be deployed at scale without prohibitive costs or complexity.

This Special Issue not only reflects current achievements but also lays out a roadmap for future research, inviting continued cross-disciplinary collaboration to address the complex and dynamic landscape of information security and data privacy.

Conflicts of Interest: No conflict of interest.

List of Contributions

1. Zhao, J.; Wu, Y.; Fu, Y.; Liu, S. ESfix: An Embedded Program Repair Tool for Effective Removal of Concurrency Defects. *Entropy* **2025**, *27*, 294. <https://doi.org/10.3390/e27030294>.
2. Zhai, Y.; Wang, T.; Zhou, Y.; Zhu, F.; Yang, B. Towards Secure Internet of Things: A Coercion-Resistant Attribute-Based Encryption Scheme with Policy Revocation. *Entropy* **2025**, *27*, 32. <https://doi.org/10.3390/e27010032>.
3. Wu, L.; Wen, Y.; Yi, J. A Higher Performance Data Backup Scheme Based on Multi-Factor Authentication. *Entropy* **2024**, *26*, 667. <https://doi.org/10.3390/e26080667>.
4. You, X.; Zhao, X.; Wang, Y.; Sun, W. Generation of Face Privacy-Protected Images Based on the Diffusion Model. *Entropy* **2024**, *26*, 479. <https://doi.org/10.3390/e26060479>.
5. Li, Y.; Xu, G.; Meng, X.; Du, W.; Ren, X. LF3PFL: A Practical Privacy-Preserving Federated Learning Algorithm Based on Local Federalization Scheme. *Entropy* **2024**, *26*, 353. <https://doi.org/10.3390/e26050353>.
6. Khatir, R.A.; Izadkhah, H.; Razmara, J. Designing a Novel Approach Using a Greedy and Information-Theoretic Clustering-Based Algorithm for Anonymizing Microdata Sets. *Entropy* **2023**, *25*, 1613. <https://doi.org/10.3390/e25121613>.
7. Ta, H.Q.; Cao, L.; Oh, H. Novel Noise Injection Scheme to Guarantee Zero Secrecy Outage under Imperfect CSI. *Entropy* **2023**, *25*, 1594. <https://doi.org/10.3390/e25121594>.

8. Kang, H.; Liu, G.; Wang, Q.; Meng, L.; Liu, J. Theory and Application of Zero Trust Security: A Brief Survey. *Entropy* **2023**, *25*, 1595. <https://doi.org/10.3390/e25121595>.

References

1. Hashmi, E.; Yamin, M.M.; Yayilgan, S.Y. Securing tomorrow: A comprehensive survey on the synergy of Artificial Intelligence and information security. *AI Ethics* **2025**, *5*, 1911–1929. [\[CrossRef\]](#)
2. Razi, Q.; Piyush, R.; Chakrabarti, A.; Singh, A.; Hassija, V.; Chalapathi, G.S.S. Enhancing Data Privacy: A Comprehensive Survey of Privacy-Enabling Technologies. *IEEE Access* **2025**, *13*, 40354–40385. [\[CrossRef\]](#)
3. Javed, Y.; Sajid, A. A Systematic Review of Privacy Policy Literature. *ACM Comput. Surv.* **2025**, *57*, 1–43. [\[CrossRef\]](#)
4. Leschanowsky, A.; Rech, S.; Popp, B.; Bäckström, T. Evaluating privacy, security, and trust perceptions in conversational AI: A systematic review. *arXiv* **2024**, arXiv:2406.09037. [\[CrossRef\]](#)
5. Yan, B.; Li, K.; Xu, M.; Dong, Y.; Zhang, Y.; Ren, Z.; Cheng, X. On protecting the data privacy of large language models (llms): A survey. *arXiv* **2024**, arXiv:2403.05156. [\[CrossRef\]](#)
6. El Mestari, S.Z.; Lenzini, G.; Demirci, H. Preserving data privacy in machine learning systems. *Comput. Secur.* **2024**, *137*, 103605. [\[CrossRef\]](#)
7. Alwahedi, F.; Aldhaheri, A.; Ferrag, M.A.; Battah, A.; Tihanyi, N. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet Things Cyber-Phys. Syst.* **2024**, *4*, 167–185. [\[CrossRef\]](#)
8. Mishra, V.; Gupta, K.; Saxena, D.; Singh, A.K. A global medical data security and privacy preserving standards identification framework for electronic healthcare consumers. *IEEE Trans. Consum. Electron.* **2024**, *70*, 4379–4387. [\[CrossRef\]](#)
9. Sheikhalishahi, M.; Saracino, A.; Martinelli, F.; La Marra, A. Privacy preserving data sharing and analysis for edge-based architectures. *Int. J. Inf. Secur.* **2022**, *21*, 79–101. [\[CrossRef\]](#)
10. Alishahi, M.; Moghtadaiee, V. Collaborative Private Classifiers Construction. In *Collaborative Approaches for Cyber Security in Cyber-Physical Systems*; Dimitrakos, T., Lopez, J., Martinelli, F., Eds.; Advanced Sciences and Technologies for Security Applications; Springer: Cham, Switzerland, 2023. [\[CrossRef\]](#)
11. Garcia, J.L.C.; Udechukwu, I.P.; Ibrahim, I.B.; Chukwu, I.J.; Dağ, H.; Dimitrova, V.; Mollakuqe, E. Securing AI systems: A comprehensive overview of cryptographic techniques for enhanced confidentiality and integrity. In Proceedings of the 2024 13th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 11–14 June 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 1–8.
12. Zhang, C.; Zhou, L.; Xu, X.; Wu, J.; Liu, Z. Adversarial attacks of vision tasks in the past 10 years: A survey. *ACM Comput. Surv.* **2024**, *58*, 1–42. [\[CrossRef\]](#)
13. Yanamala, A.K.Y.; Suryadevara, S. Navigating data protection challenges in the era of artificial intelligence: A comprehensive review. *Rev. De Intel. Artif. En Med.* **2024**, *15*, 113–146.
14. Olateju, O.; Okon, S.U.; Igwenagu, U.; Salami, A.A.; Oladoyinbo, T.O.; Olaniyi, O.O. Combating the challenges of false positives in AI-driven anomaly detection systems and enhancing data security in the cloud. *Asian J. Res. Comput. Sci.* **2024**, *17*, 264–292. [\[CrossRef\]](#)

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.