



Editorial: Sustainable Computing, Federated Intelligence, and Authentication Security

Chien-Ming Chen^{1,*}

¹School of Artificial Intelligence (School of Future Technology), Nanjing University of Information Science and Technology, Nanjing 210044, China

1 Introduction

Modern computing systems are rapidly evolving toward greater interconnection, intelligence, and decentralization. Cloud-edge infrastructures, blockchain platforms, federated learning systems, large language models, and intelligent cyber-physical applications are increasingly becoming the foundation of digital services in smart cities, transportation, industrial systems, and distributed networks. As these systems continue to expand, reliability and security are no longer isolated technical requirements, but fundamental conditions for trustworthy digital transformation.

At the same time, emerging computing paradigms are introducing new and complex challenges. Blockchain systems must address not only decentralization and consensus security, but also energy efficiency and sustainability. Federated and edge intelligence must balance model performance, privacy preservation, resource constraints, and communication efficiency. Authentication protocols for maritime transportation, drones, and other intelligent networked environments must be carefully evaluated against advanced

attacks, including key compromise, insider threats, and temporary secret leakage. These challenges demonstrate that reliable and secure computing requires both innovative system design and rigorous security analysis.

This issue of the *Journal of Reliable and Secure Computing* brings together four papers that reflect these important research directions. The selected contributions cover sustainable blockchain architecture, federated learning with large language models at the edge, and cryptanalysis of authentication protocols for emerging application scenarios. Although these studies focus on different technical problems, they share a common objective: to enhance the trustworthiness, efficiency, and resilience of modern computing systems.

By presenting these works together, this issue highlights the need to develop computing technologies that are not only intelligent and scalable, but also secure, reliable, and sustainable. We hope that the articles in this issue will provide useful insights for researchers and practitioners working on next-generation reliable and secure computing infrastructures.



Submitted: 22 June 2026

Accepted: 23 June 2026

Published: 28 June 2026

Vol. 2, No. 2, 2026.

10.62762/JRSC.2026.266725

*Corresponding author:

✉ Chien-Ming Chen

chienmingchen@ieee.org

Citation

Chen, C. M. (2026). Editorial: Sustainable Computing, Federated Intelligence, and Authentication Security. *Journal of Reliable and Secure Computing*, 2(2), 161–163.



© 2026 by the Author. Published by Institute of Central Computation and Knowledge. This is an open access article under the CC BY license (<https://creativecommons.org/licenses/by/4.0/>).

2 Papers in This Issue

The four articles included in this issue address important topics spanning sustainable blockchain systems, federated intelligence, and security analysis of authentication protocols.

The first paper, *Energy-Optimized Blockchain Architectures for Sustainable Distributed Computing*, investigates the growing concern of energy consumption in blockchain-based distributed systems [1]. The authors propose an Energy-Optimized Blockchain Architecture (EOBA) that integrates energy-aware consensus mechanisms, dynamic resource management, and carbon footprint accounting. The study demonstrates the importance of incorporating sustainability considerations into the architectural design of future blockchain infrastructures.

The second paper, *A Comprehensive Survey on Robustness and Privacy in Federated Learning Meets Large Language Model at Edge*, presents a comprehensive review of the emerging integration of federated learning and large language models within edge environments [2]. The survey examines system architectures, privacy-preserving mechanisms, deployment strategies, security challenges, and application domains. By consolidating recent advances in this rapidly evolving area, the paper provides valuable guidance for future research and development.

The third paper, *Cryptanalysis of an Authentication Protocol for Edge-Centric Maritime Transportation Systems*, performs a detailed security analysis of a recently proposed authentication protocol for maritime transportation systems [3]. The authors identify several security weaknesses, including vulnerabilities related to privileged insider attacks, temporary random number leakage attacks, and the lack of perfect forward secrecy. Their findings highlight the importance of rigorous cryptanalysis in the design of secure communication protocols.

The fourth paper, *Comments on "CSAP-IoD: A Chaotic Map-Based Secure Authentication Protocol for Internet of Drones"*, examines the security properties of a recently proposed authentication protocol for Internet of Drones environments [4]. The analysis reveals vulnerabilities to key compromise impersonation attacks and session-specific temporary random number leakage attacks. The paper further emphasizes the continuing need for robust authentication mechanisms capable of resisting

advanced adversarial models.

Taken together, these contributions reflect several important trends in contemporary computing research. While the first two papers focus on improving the efficiency, scalability, and sustainability of emerging computing paradigms, the latter two papers reinforce the critical role of security evaluation and protocol verification in ensuring trustworthy system operation. Collectively, they contribute to the broader goal of advancing reliable, secure, and sustainable computing technologies.

3 Closing Remarks

The articles presented in this issue demonstrate the diverse and rapidly evolving nature of reliable and secure computing research. From sustainable blockchain architectures and federated intelligence to the rigorous evaluation of authentication protocols, these contributions collectively highlight the growing need for computing systems that are secure, trustworthy, efficient, and resilient.

As digital infrastructures continue to expand across cloud, edge, IoT, and intelligent application environments, new challenges will emerge in areas such as cybersecurity, privacy preservation, trustworthy artificial intelligence, and sustainable computing. Addressing these challenges will require continued collaboration between researchers, practitioners, and industry stakeholders.

On behalf of the editorial team, we would like to express our sincere appreciation to all authors for their valuable contributions, to the reviewers for their time and constructive feedback, and to the members of the Editorial Board for their continued support of the journal. We hope that the research published in this issue will inspire further advances in reliable and secure computing and contribute to the development of next-generation trustworthy digital systems.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

Chien-Ming Chen served as an Editor-in-Chief of the *Journal of Reliable and Secure Computing* at the time of

manuscript submission. To ensure the integrity of the peer-review process, Chien-Ming Chen was not involved in the editorial handling, peer review, or decision-making process for this manuscript, which was handled independently by another editor.

AI Use Statement

The author declares that no generative AI was used in the preparation of this manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

- [1] Yogi, M. K., & Snehitha, J. (2026). Energy-Optimized Blockchain Architectures for Sustainable Distributed Computing. *Journal of Reliable and Secure Computing*, 2(2), 83-103. [CrossRef]
- [2] Adhikari, D., Ullah, I., Khadim, M., Hundera, N. W., Ssemwogerere, R., Debela, L. B., Jiang, W., & Xiong, H. (2026). A Comprehensive Survey on Robustness and Privacy in Federated Learning Meets Large Language Model at Edge. *Journal of Reliable and Secure Computing*, 2(2), 111-155. [CrossRef]
- [3] Liu, S., Hölbl, M., Maaliw III, R. R., & Mia, M. S. (2026). Cryptanalysis of an Authentication Protocol for Edge-Centric Maritime Transportation Systems. *Journal of Reliable and Secure Computing*, 2(2), 104-110. [CrossRef]
- [4] Kumar, A., & Kumari, S. (2026). Comments on CSAP-IoD: A Chaotic Map-Based Secure Authentication Protocol for Internet of Drones. *Journal of Reliable and Secure Computing*, 2(2), 156-160. [CrossRef]



Chien-Ming Chen Editor-in-Chief of Journal of Reliable and Secure Computing. (Email: chienmingchen@ieee.org)