EDITORIAL

Inaugural Editorial for the *Journal of Reliable and Secure Computing*

Chien-Ming Chen[1,*], **Kuo-Hui Yeh**[2], **Saru Kumari**[3] **and Hu Xiong**[4]

[1] School of Artificial Intelligence (School of Future Technology), Nanjing University of Information Science and Technology, Nanjing 210044, China
[2] National Yang Ming Chiao Tung University, Hsinchu 300, Taiwan
[3] Chaudhary Charan Singh University, Meerut 250004, India
[4] School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

1 Introduction: Why This Journal and Why Now?

The digital world is entering an era of unprecedented complexity. From cloud computing to edge intelligence, from blockchain to the metaverse, and from cyber–physical systems to large scale artificial intelligence (AI), the infrastructures that shape our society are becoming increasingly interconnected and interdependent. These advances create enormous opportunities; however, they also pose formidable challenges in ensuring that systems remain reliable, trustworthy, and secure. Reliability failures or cybersecurity breaches are no longer isolated technical issues. They can disrupt economies, compromise critical infrastructures, and erode public trust.

In this context, the *Journal of Reliable and Secure Computing* (*JRSC*) has been launched to provide an international, peer reviewed platform that directly addresses these urgent challenges. The *JRSC* is dedicated to publishing high-quality research that integrates foundational theories, emerging technologies, and practical solutions to support the development of resilient and trustworthy digital ecosystems.

2 Objectives of *JRSC*

The mission of the *JRSC* can be summarized in three main objectives.

1. *JRSC* seeks to advance fundamental research on reliability, trust, and security in computing systems. It aims to provide rigorous theoretical frameworks as well as innovative methodologies.
2. *JRSC* is designed to bridge disciplinary boundaries across computing, communication, cryptography, and artificial intelligence. By promoting collaboration across fields that have often evolved separately, the journal fosters cross pollination of ideas and solutions.
3. *JRSC* aspires to serve as a global knowledge hub for both academic researchers and industry practitioners. It provides a venue for the exchange of ideas, the dissemination of best practices, and

Submitted: 24 September 2025
Accepted: 25 September 2025
Published: 29 September 2025

Vol. 1, **No.** 1, 2025.
10.62762/JRSC.2025.220451

***Corresponding author:**
✉ Chien-Ming Chen
chienmingchen@ieee.org

Citation
Chen, C. M., Yeh, K. H., Kumari, S., & Xiong, H. (2025). Inaugural Editorial for the Journal of Reliable and Secure Computing. *Journal of Reliable and Secure Computing*, 1(1), 1–3.

the exploration of cutting-edge solutions that ensure secure and dependable systems.

Through these objectives, the *JRSC* aims to foster a strong international community committed to shaping the future of reliable computing.

3 Scope of the Journal

The *JRSC* welcomes original research papers, surveys, and case studies covering a broad range of topics, including but not limited to:

1. Dependable and fault-tolerant computing: Theories, models, and systems that ensure robustness in the presence of failures, attacks, or adversarial conditions.
2. System verification and resilience: Formal methods, testing, and self-healing systems that maintain stability and correctness.
3. Cybersecurity and privacy technologies: Cryptographic protocols, authentication mechanisms, privacy-preserving computation, and compliance frameworks.
4. AI for security and security for AI: Adversarial machine learning, trustworthy AI, explainability, and intelligent threat detection.
5. Secure architectures and infrastructures – cloud, edge, IoT, blockchain, digital twins, and metaverse platforms.
6. Applied and industrial perspectives: Case studies in critical infrastructures, national security, healthcare, transportation, and smart cities.

This scope reflects the ambition of the *JRSC* to provide a comprehensive and interdisciplinary space, addressing both the theoretical underpinnings and the real-world applications of reliable and secure computing.

4 Current Trends and Research Challenges

The research community is witnessing several transformative trends that make the *JRSC*'s mission especially timely:

1. Trustworthy AI: As AI permeates critical applications such as autonomous vehicles, healthcare diagnostics, and financial decision making, ensuring robustness against adversarial attacks, fairness in decision-making, and transparency in reasoning has become vital [1, 2].
2. Privacy and Post-Quantum Cryptography: The advent of quantum computing poses risks to current cryptographic systems, accelerating research on post-quantum cryptography. Simultaneously, privacy-preserving methods such as federated learning and differential privacy are gaining traction in large-scale data ecosystems [3, 4].
3. Dependability in Complex Systems: With the rise of cyber–physical systems and digital twins, maintaining dependability across highly complex and distributed systems is a formidable challenge. Formal verification, runtime monitoring, and resilience engineering are increasingly critical [5].
4. Security of Emerging Infrastructures: From blockchain to 6G-enabled IoT systems, new infrastructures bring both opportunities and vulnerabilities. Attack surfaces are expanding, demanding new paradigms for security and compliance [6, 7].

Addressing these challenges requires innovation, strong collaboration, and true interdisciplinarity. These principles are central to the mission of the *JRSC*.

5 Vision for the Future

The *JRSC* envisions becoming a leading journal that defines the discourse on reliable and secure computing. Over the next few years, we aim to:

1. Build a strong international editorial board of distinguished scholars and practitioners.
2. Maintain rigorous peer review standards to ensure academic excellence.
3. Encourage submissions that combine theoretical innovation with practical impact.
4. Gradually achieve recognition in indexing platforms such as Scopus and Web of Science, paving the way for broader visibility and influence.

Above all, the *JRSC* will grow through the collective efforts of the community. We warmly invite researchers to submit their high-quality work, serve as reviewers, and join us as editorial board members. Together, we can shape the *JRSC* into a trusted venue that reflects the evolving needs of our field.

6 Closing Remarks

The launch of the *Journal of Reliable and Secure Computing* reflects a shared belief that reliability, trust, and security are essential attributes of digital systems. *JRSC* aims to become a vibrant forum that advances knowledge, inspires innovation, and strengthens collaboration across disciplines.

We warmly welcome the contributions of researchers worldwide to make the *JRSC* a recognized and impactful journal in the coming years.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Chander, B., John, C., Warrier, L., & Gopalakrishnan, K. (2025). Toward trustworthy artificial intelligence (TAI) in the context of explainability and robustness. *ACM Computing Surveys, 57*(6), 1-49. [CrossRef]

[2] Methnani, L., Chiou, M., Dignum, V., & Theodorou, A. (2024). Who's in charge here? a survey on trustworthy ai in variable autonomy robotic systems. *ACM computing surveys, 56*(7), 1-32. [CrossRef]

[3] Mansoor, K., Afzal, M., Iqbal, W., & Abbas, Y. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing, 28*(2), 93. [CrossRef]

[4] Gharavi, H., Granjal, J., & Monteiro, E. (2024). Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Communications Surveys & Tutorials, 26*(3), 1748-1774. [CrossRef]

[5] Amiri, Z., Heidari, A., Navimipour, N. J., & Unal, M. (2023). Resilient and dependability management in distributed environments: A systematic and comprehensive literature review. *Cluster Computing, 26*(2), 1565-1600. [CrossRef]

[6] Shokry, M., Awad, A. I., Abd-Ellah, M. K., & Khalaf, A. A. (2022). Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. *Future Generation Computer Systems, 136*, 358-377. [CrossRef]

[7] Khoshafa, M. H., Maraqa, O., Moualeu, J. M., Aboagye, S., Ngatched, T. M., Ahmed, M. H., ... & Di Renzo, M. (2024). RIS-assisted physical layer security in emerging RF and optical wireless communication systems: A comprehensive survey. *IEEE Communications Surveys & Tutorials*. [CrossRef]

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

Kuo-Hui Yeh Editor-in-Chief of *Journal of Reliable and Secure Computing*. (Email: khyeh@nycu.edu.tw)

Saru Kumari Co-Editor-in-Chief of *Journal of Reliable and Secure Computing*. (Email: saryusiirohi@gmail.com)

Hu Xiong Co-Editor-in-Chief of *Journal of Reliable and Secure Computing*. (Email: xionghu@uestc.edu.cn)