Asia Pacific Science Press

Journal of Cyber Security and Intelligent Systems
ISSN(O): 3135-1158
ISSN(P): 3135-114X
Vol. 1 No.1 (2026)
DOI: https://doi.org/10.62177/jcsis.v1i1.1606

Editor's Foreword

Dear Scholars, Researchers, Engineers, Practitioners, and Esteemed Readers,

Digital systems now mediate an extraordinary share of modern life. They support public services, scientific discovery, industrial production, financial activity, healthcare, communication, and personal exchange. At the same time, intelligence is becoming deeply embedded in these systems. Machine learning models assist perception and prediction; autonomous components make decisions at speed; and connected infrastructures continuously adapt to changing environments. These capabilities bring remarkable opportunities, but they also enlarge the surface on which failures, attacks, misuse, and unintended consequences can occur.

Cybersecurity and intelligent computing can therefore no longer be treated as separate domains. Intelligent technologies are transforming defense through automated detection, behavioral analysis, adaptive response, and threat forecasting. Yet the same technologies may be manipulated through adversarial inputs, poisoned data, model extraction, deceptive content, or exploitation of opaque decision processes. Security must be designed not only around networks and software, but also around data, models, agents, human behavior, and the complex interactions among them. Conversely, intelligent systems cannot be considered genuinely advanced if they are fragile, unaccountable, or unsafe in the environments in which they operate.

The *Journal of Cyber Security and Intelligent Systems* (JCSIS) is founded in response to this convergence. It is an international academic journal dedicated to advancing the theory, methodology, engineering, and practical application of secure information systems and intelligent technologies. Our purpose is to create a forum where cybersecurity researchers, artificial intelligence specialists, systems engineers, and practitioners can address common problems, exchange methods, and develop solutions that are both technically effective and socially responsible.

The journal welcomes work across a broad range of topics, including network and system security, cryptography, privacy-preserving computation, software and hardware security, authentication and access control, cloud-edge security, Internet of Things security, digital forensics, threat intelligence, malware analysis, secure architectures, and critical-infrastructure protection. Within intelligent systems, we invite contributions on trustworthy machine learning, adversarial robustness, explainability, intelligent intrusion detection, adaptive defense, secure autonomous systems, privacy-aware data intelligence, human-centered security, and resilient decision-making. We are especially interested in research that addresses the points at which these areas intersect.

JCSIS seeks contributions that connect sound ideas with convincing evidence. This includes theoretical studies that clarify security properties or limitations; methodological work that introduces new models, algorithms, protocols, or evaluation frameworks; and applied research that demonstrates how a system performs under realistic operational conditions. Negative findings, carefully designed benchmarks, reproducibility studies, and analyses of failure modes can be as valuable as reports of improved

performance. Security research advances when the community understands not only what works, but also what breaks, under which assumptions, and at what cost.

Four principles will shape our editorial direction. First, rigor: claims should be supported by appropriate threat models, baselines, experiments, proofs, or field evidence. Second, resilience: proposed systems should be assessed under uncertainty, adaptation, and adversarial pressure rather than only under ideal conditions. Third, responsibility: authors should consider privacy, fairness, safety, dual-use risks, and the human consequences of deployment. Fourth, openness: progress depends on dialogue across disciplines and sectors, including collaboration among universities, industry, government, and professional communities.

These principles are particularly important because cybersecurity is an applied science with immediate consequences. A technique that performs well in a laboratory may encounter different constraints in a hospital, transport system, industrial plant, public network, or small organization. An intelligent defense mechanism may improve detection while introducing new dependencies or false positives. JCSIS encourages authors to make these trade-offs visible. We welcome research that takes deployment context seriously, reports limitations candidly, and identifies pathways from prototypes to systems that can be trusted in practice.

The journal also aims to support an inclusive international research community. Cyber threats cross borders, but technical capacity, infrastructure, regulation, and exposure to risk vary considerably. Insights from different regions and operating environments can reveal assumptions that remain invisible in a single context. We invite comparative research, interdisciplinary perspectives, and contributions that address the security needs of both advanced and resource-constrained settings. By bringing diverse experience into a shared conversation, the field can develop solutions that are more robust and more broadly useful.

We warmly invite scholars, engineers, practitioners, and policymakers to contribute original research, critical reviews, system studies, and forward-looking perspectives. We also invite members of the community to serve as reviewers and to help us uphold a peer-review process that is exacting, fair, constructive, and timely. The quality of JCSIS will depend on the care with which authors frame problems, reviewers test claims, and readers carry ideas into new settings.

With the inaugural issue, we begin with a clear aspiration: to make JCSIS a trusted platform for research that strengthens digital security while advancing intelligent capability. The challenge before us is not merely to build systems that can compute and adapt, but to build systems worthy of reliance. On behalf of the editorial team, I thank everyone whose scholarship and service will shape this endeavor, and I look forward to the discoveries and collaborations ahead.

Journal of Cyber Security and Intelligent Systems (JCSIS)
Editor-in-Chief: Dr. Fangzhou Song