Journal of Machine Learning and Information Security
https://www.sciltp.com/journals/jmlis

Editorial

Inaugural Issue for Journal of Machine Learning and Information Security

Xiaofeng Liao [1,2]

[1] Department of Computer Science, Chongqing University, Chongqing 400044, China; xfliao2025@126.com;
[2] Key Laboratory of Dependable Services Computing in Cyber Physical Society-Ministry of Education, Chongqing 400044, China

How To Cite: Liao, X. Inaugural Issue for Journal of Machine Learning and Information Security. *Journal of Machine Learning and Information Security* **2025**, *1*(1), 1.

It has been my great pleasure to introduce you the inaugural issue for *Journal of Machine Learning and Information Security* (*JMLIS*), which serves as one of the world's premier journals for disseminating cutting-edge research in the broad domains of advanced machine learning and information security and aims to bridge the gap between theoretical research and practical implementation. It covers feature, perspective and review articles, alongside original research, focusing on the advanced theories and practical applications in mathematics, computer science, electronic information, industrial engineering, control science, communication engineering, and other fields, which is anticipated to serve as the hub for sharing knowledge among researchers.

Machine learning has become a foundational technology for modeling complex, high-dimensional data across domains. Advances in deep learning, representation learning, and reinforcement learning have enabled systems to achieve superhuman performance in perception, prediction, and decision-making tasks. From supervised classification to self-supervised pre-training on large-scale datasets, machine learning models are now integral to applications in natural language processing, computer vision, and autonomous systems. However, their data-driven nature introduces challenges related to generalization, interpretability, and robustness—particularly when deployed in dynamic, real-world environments. Concurrently, information security has fundamentally shifted from a perimeter-defense model to a dynamic, data-centric challenge. The discipline is characterized by a continuous arms race against increasingly sophisticated and persistent adversaries. Modern security focuses on protecting systems' confidentiality, integrity, and availability against advanced persistent threats, ransomware, and large-scale vulnerabilities in complex software supply chains. The paradigm has moved towards continuous monitoring, threat intelligence integration, and developing resilient architectures capable of operating under attack, acknowledging that prevention alone is insufficient. The integration of machine learning and information security is driving transformative advances across both fields. Machine learning offers powerful capabilities for large-scale threat detection, behavioral analysis, and automated response, enabling systems to identify novel attacks, classify malware, and predict vulnerabilities with unprecedented speed and accuracy. In turn, the demanding requirements of security applications are stimulating new developments in machine learning—particularly in areas such as robust, interpretable, and privacy-aware learning. Adversarial environments have spurred innovations in model resilience, transparency, and adaptive inference. This synergistic partnership not only enhances cyber defense but also fosters foundational progress in machine learning itself, paving the way for more trustworthy and effective intelligent systems in critical applications.

The *Journal of Machine Learning and Information Security* (*JMLIS*) has an intentionally broad scope, aiming to embrace original and pioneering fundamental research at the intersection of machine learning and information security and shape the future of secure and intelligent computing. We invite researchers, engineers, and industry experts to contribute high-quality original research papers and comprehensive review articles that contribute to theoretical advancements, novel methodologies, and real-world applications in these fields. Our journal serves as a platform for researchers and practitioners to explore innovative solutions that enhance the security, robustness, and efficiency of machine learning models, as well as the application of artificial intelligence driven techniques in cybersecurity. *JMLIS* accepts a wide range of academic manuscripts, including original research articles, reviews, and communications, covering topics such as, but not limited to:

- ✧ Machine Learning for Security: Adversarial machine learning; Secure federated learning; Privacy-preserving artificial intelligence models; Trust and fairness in artificial intelligence.
- ✧ Security for Machine Learning: Robust model training; Secure data sharing and encryption for machine learning; Artificial-intelligence-driven intrusion detection and threat mitigation.
- ✧ Privacy and Data Protection: Cloud security; Blockchain for data privacy; Differential privacy techniques; Access control and authentication.
- ✧ Image and Signal Security: Secure image encryption and transmission; Artificial-intelligence-based blind image denoising; Image quality evaluation for forensic analysis.
- ✧ Intelligent Systems and Network Security: Reinforcement learning for secure intelligent systems; Cooperative control in cybersecurity; Networked system optimization with artificial-intelligence.

This inaugural issue captures a timely and significant snapshot of current advancements in the area of machine learning and information security. In June 2025, I invited a distinguished cohort of researchers to join the editorial board, and I am deeply grateful for their commitment and expert guidance in launching this rigorous scholarly endeavor. I extend my sincere appreciation to all contributing authors for their exceptional work and dedication to producing high-quality, impactful research. I also acknowledge the invaluable contributions of the peer reviewers, whose meticulous and prompt evaluations are instrumental in ensuring the scientific integrity and excellence of this issue. Finally, my profound thanks go to the editorial and production team at Scilight Press for their unwavering support, professional expertise, and steadfast collaboration in bringing this inaugural volume to fruition.

Conflicts of Interest

The author declares no conflict of interest.