Journal of Universal Computer Science, vol. 32, no. 9 (2026), 1258-1260
submitted: 23/7/2026, accepted: 24/7/2026, appeared: 14/9/2026 CC BY 4.0

Editorial: Artificial Intelligence-Driven Information Security and Privacy Enhancement Technologies

J.UCS Special Issue

Jingsha He
(Beijing University of Technology, Beijing, China
https://orcid.org/0000-0002-8122-8052, jsh.bjut@gmail.com)

Dragan Peraković
(University of Zagreb, Zagreb, Croatia
https://orcid.org/0000-0002-0476-9373, dragan.perakovic@fpz.hr)

Biplob Ray
(CQ University, Rockhampton, Australia
https://orcid.org/0000-0002-3016-1695, b.ray@cqu.edu.au)

The rapid development of digitalization and intelligent computing has reshaped the technical foundations of information systems, data services, industrial platforms, and networked infrastructures. At the same time, it has also intensified the risks associated with information security, privacy protection, and trustworthy data processing. Generative artificial intelligence, large-scale data analytics, distributed computing, cloud services, Internet of Things systems, and edge intelligence have introduced new opportunities for automated defense, intelligent monitoring, and privacy-preserving computation. However, these technologies also create new attack surfaces, increase system complexity, and challenge conventional security mechanisms that rely mainly on static rules, predefined signatures, or isolated protection models.

The Special Issue on Artificial Intelligence-Driven Information Security and Privacy Enhancement Technologies focuses on recent research at the intersection of artificial intelligence, cybersecurity, privacy protection, cryptographic technologies, secure computation, and intelligent system defense. The motivation of this special issue lies in the need to develop more adaptive, verifiable, scalable, and privacy-aware security mechanisms for increasingly complex digital environments. In particular, AI-driven methods have the potential to improve malicious code detection, vulnerability discovery, fuzz testing, network attack detection, cryptographic computation, zero-knowledge verification, and privacy-preserving distributed learning. These research directions are particularly important as modern information systems must simultaneously address security effectiveness, computational efficiency, privacy compliance, and deployment feasibility.

This special issue was organized as an open call and was not associated with any conference. In total, 44 submissions were received. Each accepted paper received at least three reviews. After the first round of peer review, 36 submissions were rejected. The remaining eight papers underwent a second round of review and revision, during which the authors were required to respond carefully to the reviewers' comments. After

further editorial assessment, two additional papers were rejected because of possible potential risks identified during the final review stage. As a result, six papers were finally accepted for inclusion in this special issue.

We would like to thank all authors who submitted their work to this special issue. We also sincerely thank all reviewers for their time, expertise, and constructive comments, which were essential to maintaining the academic quality of the issue. We are grateful to the J.UCS editorial team for their support throughout the preparation and publication process. We hope that this special issue will provide readers with useful insights into emerging AI-driven methods for information security and privacy enhancement.

Jingsha He, Dragan Peraković & Biplob Ray

Papers in this Special Issue

The following six papers have been included in this special issue.

Shaofeng Ming, Ying Ling, Xin Li, Songming Han, Zhengwang Miao, and Xizheng Pan present "Malicious Code Detection Based on AST Multi-dimensional Feature Fusion and Dynamic Graph Optimization." The paper proposes a malicious code detection method that combines abstract syntax tree-based feature fusion with dynamic graph optimization. By integrating syntactic and semantic code representations and adaptively optimizing graph structures, the method improves the detection of complex malicious behaviors and demonstrates strong performance on the Ember dataset.

Ziyi Xu contributes "Veritas Gateway: A Framework for Zero-Knowledge Proofs on Database Queries with a Model Context Protocol Interface." The paper introduces a zero-knowledge verification layer for database queries in AI-agent workflows. Through Merkle commitments and succinct proofs, the framework enables locally verifiable query results across heterogeneous databases without exposing raw data, supporting trustworthy and privacy-sensitive data access.

Shaoguang Wu, Jiyou Chang, Jiannan Guo, Fang Chen, Hongchang Wei, Zhijuan Wang, Guanghua Zhang, and Yijie Chu present "SKAEG: Automatic Exploit Generation Based on Shared Keywords in Embedded Systems." The paper proposes an automatic exploit generation framework for IoT firmware vulnerabilities. By using shared keywords to guide vulnerability analysis, exploitability assessment, and request construction, SKAEG improves the efficiency of exploit generation for embedded systems and validates its effectiveness across multiple IoT devices.

Shiguang Guo and Zhihao Liu contribute "The Dynamic Optimization of AFL Fuzzing Mutation Strategies Based on Adaptive Reward Proximal Policy Optimization." The paper improves AFL fuzzing by incorporating an adaptive reward mechanism into the Proximal Policy Optimization framework. The proposed approach dynamically guides mutation strategy selection according to fuzzing feedback, leading to better code coverage and vulnerability discovery than traditional AFL and standard PPO methods.

Dingxing Xie, Xiaochuan Hu, Lin Peng, Gencheng Liu, Naijun Cheng, Jie Liu, and Yang Zhang present "Optimization of Parallel Number Theoretic Transform Algorithms for Multi-Core Digital Signal Processors." The paper develops an optimization framework for accelerating Number Theoretic Transform algorithms on

multi-core digital signal processors. Through algorithmic decomposition, SIMD-aware microkernel design, vectorized modular multiplication, and pipelined execution, the work provides an efficient implementation strategy for cryptographic and signal-processing applications.

Xin Liu and Xiang Liu contribute "A Spatio-Temporal Transformer-Based Approach for Network Attack Detection." The paper proposes a privacy-preserving network attack detection framework for dynamic environments such as IoT and Vehicle-to-Everything networks. By combining adaptive spatio-temporal graph generation, Transformer-based modeling, federated learning, and dynamic defense adjustment, the approach improves real-time threat detection while reducing privacy risks.

Reviewers of this Special Issue

Bi-sheng ZHAN, Huazhong University of Science and Technology
Dawei Xu, Changchun University
Fangyu Li, Beijing University of Technology
Guigang Zhang, Institute of Automation Chinese Academy of Sciences
Guowei Wang, Jilin Engineering Normal University
Haiming Liu, University of Southampton
Hantao Liu, Cardiff University
Hongwu Lv, Harbin Engineering University
Jianbo Chen, Fuzhou Institute of Technology
Jing Ge, Central China Normal University
Lina Yuan, Tongren University
Quanrong Fang, Zhejiang University
Ruizhong Du, Hebei University
Ruyi Dong, Jilin University of Chemical Technology
Teng Cheng, The Hefei University of Technology
Vatsal Gupta, Apple Inc.
Wei Zhang, Xianyang Normal University
Wuman Luo, Macao Polytechnic University
Xiangyu Meng, Louisiana State University
Xiaoyi Zhou, Hainan University
Xiaoyong Bo, JiLin Agricultural Science and Technology University
Xinli Li, North China Electric Power University
Yin Li, Dongguan University of Technology
Yingying Yin, Jilin Agricultural University