CALL FOR PAPERS

IEEE Internet of Things Journal

Special Issue on AI-Driven Network Forensics for Edge-Intelligent Internet of Things

The rapid integration of Artificial Intelligence (AI) into Internet of Things (IoT) networks is transforming sensing, communication, and decision-making at the edge. While AI-enabled IoT systems enhance operational efficiency, they introduce new challenges in accountability, incident explanation, and post-event analysis. In large-scale heterogeneous IoT deployments, many devices lack reliable logging capabilities, making traditional host-centric security mechanisms insufficient for reconstructing failures or cyber-attacks. This creates a growing need for network-centric forensics, where the network and edge infrastructure itself serves as a primary source of trustworthy evidence.

This Special Issue focuses on AI-driven, network-centric forensics for edge-intelligent IoT systems, emphasizing post-incident reconstruction and accountability. Authors are invited to submit original research on forensic-ready networking architectures and intelligent evidence acquisition mechanisms that enable threat identification, evidence correlation, and causal attribution.

- Forensic architectures and protocols for evidence acquisition in AI-enabled IoT networks
- Adaptive resource allocation for evidence utility and storage efficiency in IoT forensics
- Agentic AI-based traffic-level threat identification and classification in IoT networks
- LLM-assisted provenance modeling and causal graph construction in IoT networks
- Intelligent forensic knowledge abstraction and correlation across heterogeneous IoT networks
- AI-enabled immutable chain-of-custody and secure provenance for tamper-proof evidence and legal accountability in edge environments
- Cross-domain forensic architectures using federated learning and privacy-enhancing technologies for fragmented IoT networks
- Scalable Forensics-as-a-Service with edge-assisted monitoring for mission-critical IoT systems
- Large action model enabled automated forensic workflow orchestration and active evidence probing in IoT systems
- Energy-efficient and hardware/software co-design for network-centric forensics in edge-intelligent IoT systems
- Explainable AI (XAI) and admissibility-aware analysis for interpretable evidence and legal attribution in IoT networks
- Experimental evaluation and benchmarks for IoT forensics using real-world testbeds, realistic traces, and forensic-specific metrics

Important Dates

- Submission Deadline: October 31st, 2026
- First Review Due: November 15th, 2026
- Revision Due: December 15th, 2026
- Second Reviews Due/Notification: January 15th, 2027
- Final Manuscript Due: April 30th, 2027
- Publication Date: June, 2027

Submission

The original manuscripts to be submitted need to follow the guidelines at: https://ieee-iotj.org/wp-content/uploads/2025/02/IEEE-IoTJ-Author-Guidelines.pdf, which should not be concurrently submitted for publication in other venues. Authors should submit their manuscripts through the IEEE Author Portal at: https://ieee.atyponrex.com/journal/iot. The authors must select as "Special Issue on AI-Driven Network Forensics for Edge-Intelligent Internet of Things" when they reach the "Article Type" step in the submission process.

Guest Editors

- Jialing He, Chongqing University, China (hejialing@cqu.edu.cn)
- Akhilesh S. Thyagaturu, Intel Corporation, USA (athyagat@asu.edu)
- Marco Di Renzo, CNRS-CentraleSupelec, France and King's College London, UK (marco.di_renzo@kcl.ac.uk)
- Sinem Coleri, Koc University, Turkey (scoleri@ku.edu.tr)
- Tao Xiang, Chongqing University, China (txiang@cqu.edu.cn)