CALL FOR PAPERS

IEEE Internet of Things Journal

Special Issue on Security and Privacy in Large Language Models for Internet of Things (IoT)

Large Language Models (LLMs) such as ChatGPT have revolutionized many aspects of modern life with their powerful generation, contextual understanding, and multi-modal processing. Meanwhile, the rapid advances of Internet of Things (IoT) devices have led to the proliferation of smart devices from the home to the industrial. These devices are equipped with advanced sensors and communication technologies that can collect and transmit large amounts of data. Combining these IoT devices with LLMs not only enhances communication capabilities, but also creates a new interaction paradigm that efficiently integrates human needs with machine intelligence, significantly improving efficiency and quality of intelligent services.

The combination of LLMs and IoT devices brings intelligence to the devices, but also data security and privacy issues. However, it is challenging to safeguard the security and privacy of these devices due to the IoT devices variety, the complex structure of LLMs, and the diversity of data. To address these challenges, this special issue collects the latest research outcomes and developments on the security, privacy and trust in combination of LLMs and IoT devices. Topics of interest include but are not limited to:

- LLMs-Enhanced Authentication for IoT Devices
- LLMs-Based Access Control for IoT
- LLMs for Truth Verification in IoT Sensing
- LLMs for Data Privacy in IoT Cloud Services
- Federated LLMs Learning in IoT Security
- LLMs-Driven Trust Management for IoT
- Blockchain and LLMs Convergence for IoT Security
- Edge-Deployed LLMs Security in IoT
- Incentive Strategies for LLMs Interaction in IoT
- LLMs Applications for Smart City IoT Security

Important Dates:

- Submission Deadline: April 15th, 2025
- First Review Due: May 30th, 2025
- Revision Due: July 15th, 2025

- Second Reviews Due/Notification: August 15th, 2025
- Final Manuscript Due: October 30th, 2025
- Publication Date: January 2026

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 "SI: Security and Privacy in Large Language Models for Internet of Things (IoT)" when they reach the "Article Type" step in the submission process.

Guest Editors:

- Haomiao Yang, University of Electronic Science and Technology of China, China (haomyang@uestc.edu.cn)
- Tianwei Zhang, Nanyang Technological University, Singapore (tianwei.zhang@ntu.edu.sg)
- Rongxing Lu, University of New Brunswick, Canada (RLU1@unb.ca)
- Hyunsung Kim, Kyungil University, Kyungbuk, Korea (kim@kiu.ac.kr)
- Kuan Zhang, University of Nebraska–Lincoln, United States (kuan.zhang@unl.edu)