Title： Privacy and Security Mechanisms for Federated Learning in IoT Systems

Organizers:

Ying Gao, South China University of Technology, gaoying@scut.edu.cn

Wing W. Y. Ng, South China University of Technology, wingng@ieee.org

Xingfu Yan, South China Normal University, xfyan78@163.com

William Yijiang Li, University of California San Diego, yijiangli@ucsd.edu

Abstract

The proliferation of Internet of Things (IoT) devices and the increasing demand for privacy-aware intelligence at the edge have led to the widespread adoption of federated learning (FL) in resource-constrained environments. FL enables collaborative model training across decentralized clients—such as smart sensors, wearable devices, and autonomous vehicles—without transferring sensitive raw data to centralized servers. This paradigm holds strong potential for next-generation AI applications in healthcare, smart homes, transportation, and industrial automation. However, the intersection of FL and IoT introduces a complex and evolving landscape of security and privacy risks.

Unlike traditional cloud-centric architectures, IoT environments are inherently decentralized, heterogeneous, and bandwidth-limited. Devices participating in federated learning often vary widely in computational power, data quality, and connectivity, making them vulnerable to a wide range of attacks including inference attacks, poisoning, model inversion, and malicious aggregation. Furthermore, ensuring robust privacy protection—while preserving learning utility—remains a central challenge in real-world deployments.

This special session seeks to bring together researchers and practitioners to explore innovative solutions that enhance the security and privacy of federated learning in IoT ecosystems. We invite original research, system designs, and visionary perspectives that advance the theoretical understanding, practical implementation, and cross-domain integration of privacy-preserving techniques in federated IoT settings. Topics of interest include, but are not limited to:

Topics of Interest

* Privacy-preserving federated learning protocols for IoT
* Secure aggregation and model update authentication in FL
* Lightweight cryptographic techniques for IoT-FL environments
* Data poisoning and backdoor attacks in FL-enabled IoT systems
* Secure model personalization and transfer learning in FL
* Adversarial robustness in federated IoT networks
* Blockchain and distributed ledger technologies for trustworthy FL
* Identity management and access control in FL-IoT settings
* Trust management and reputation systems in federated IoT systems
* Communication-efficient secure FL under IoT constraints
* Privacy-aware task allocation and resource management in federated IoT
* Federated learning for healthcare, smart home, and industrial IoT applications