CALL FOR PAPERS

IEEE Internet of Things Journal

Special Issue on Federated Unlearning and Model Governance for Trustworthy IoT: Selective Forgetting, Provenance, and Auditability at the Edge

Federated learning enables distributed IoT devices to train shared models without exporting raw data. Yet, once data has influenced a global model, its effects persist across parameters, aggregation rounds, and subsequent versions. Current federated architectures lack principled mechanisms to remove this influence when consent is withdrawn, devices are decommissioned, assets change ownership, poisoned contributions are detected, or regulators require proof of deletion. Retraining from scratch for every request is impractical at IoT scale. This challenge is also regulatory. Data deletion rights are established under frameworks such as China's PIPL, the CCPA, India's DPDP Act, and the GDPR, with further obligations emerging from the EU AI Act. Compliance therefore requires lifecycle-wide mechanisms to trace, remove, verify, and audit data influence. This Special Issue invites original contributions on federated unlearning and model governance in IoT environments. We seek approaches that treat forgetting as a core system requirement while addressing resource constraints, intermittent participation, device heterogeneity, non-IID data, and the impracticality of centralised retraining. We particularly welcome deployable solutions that quantify energy and communication costs and provide rigorous verification of unlearning beyond proxy metrics.

Topics of interest include, but are not limited to:

- Efficient and granular federated unlearning under IoT resource constraints, including client-, sample-, class-, and feature-level forgetting, with attention to energy, latency, and communication costs
- Verification, certification, and reproducible evaluation of federated unlearning through formal guarantees, defensible auditing procedures, benchmarks, and datasets
- Privacy and security implications of unlearning, including membership inference, model inversion, reconstruction attacks, and recovery from poisoned or corrupted contributions
- Update provenance, model lineage, contribution attribution, consent lifecycle management, revocation propagation, and policy enforcement across federated IoT systems
- Federated unlearning under non-IID data, partial participation, client dropout, asynchronous aggregation, and vertical, hierarchical, or cross-silo architectures
- Regulatory alignment, on-device foundation-model editing, and real-world applications in healthcare, connected vehicles, industrial IoT, wearables, and smart infrastructure

Important Dates

- Submission Deadline: 15 March 2027
- First Review Due: 31 May 2027
- Revision Due: 15 July 2027
- Final notification: 15 August 2027
- Final Manuscripts Due: 15 September 2027
- Publication date: Novembre 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 "**Federated Unlearning and Model Governance for Trustworthy IoT: Selective Forgetting, Provenance, and Auditability at the Edge**" when they reach the "Article Type" step in the submission process.

Guest Editors

Francesco Piccialli (Lead), University of Naples Federico II, Italy · francesco.piccialli@unina.it
David Camacho, United Arab Emirates University, EAU
Sadi Alawadi, Blekinge Institute of Technology, Sweden
Rehmat Ullah, Newcastle University, United Kingdom
Kenli Li, Hunan University, China
Xiaohua Tony Hu, Drexel University, United States