Title: FLEX-IDS: A secure and explainable federated intrusion detection framework for Edge-of-Things environments under adversarial conditions

Author names: Abrity Paul Chowdhury , Fernaz Narin Nur , A.H.M. Saiful Islam , Khorshed Alam , Asif Karim , Mohd Asif Shah

Abstract: The convergence of the Internet of Things (IoT) with edge computing has created the Edge of Things (EoT), enabling real-time analytics but also expanding the cyber-attack surface. Traditional centralized Intrusion Detection Systems (IDS) are ill-suited for such decentralized, latency-sensitive environments. This paper presents **FLEX-IDS**, a federated, explainable, and adversarially robust IDS framework for heterogeneous EoT networks. FLEX-IDS combines five federated optimizers (FedAvg, FedOpt, FedProx, FedNova, FedPer) with cryptographic safeguards and post-hoc interpretability (SHAP and LIME) to ensure privacy, resilience, and transparency. Evaluated on three benchmark datasets **CICIDS2017**, **UNSW-NB15**, and **ToN-IoT**, the system achieves up to **98.05% accuracy** and maintains a mean F1-score of **0.86** under 30% malicious participation. FLEX-IDS demonstrates energy efficiency (**0.03–0.16 J/round**) and edge-feasible explainability, achieving SHAP fidelity of **0.97**. These results highlight FLEX-IDS as a scalable, secure, and interpretable intrusion detection solution for next-generation IoT infrastructures.

Keywords: Federated learning Intrusion Detection System Edge of Things (EoT) Adversarial robustness Explainable artificial intelligence IoT security

https://doi.org/10.1016/j.compeleceng.2025.110827