IEEE Africon, Protea Hotel Polokwane Ranch Resort, Polokwane, 10-12 December 2025

Analysis of privacy-preserving federated learning's resilience against adverse attacks in Internet of Things systems

Molose, R; Isong, B; Abu Mahfouz, Adnan MI; Dladlu, N

Abstract

Federated Learning (FL) enables Internet of Things (IoT) devices to learn from decentralized data, enhancing privacy, security, and efficiency. However, its vulnerability to adversarial attacks poses significant challenges. This paper evaluates various FL models: Hierarchical FedAvg, Decentralized FedAvg (D-FedAvg), Alternating Direction Method of Multipliers (ADMM), Gossip Learning (GL), and Stochastic Gossip Learning (SGL), for anomaly detection in network traffic. We utilize NSL-KDD datasets and metrics such as accuracy, communication overhead, and computation time to analyse their performance under normal and adversarial conditions. The findings reveal that Hierarchical FedAvg achieves the highest accuracy (93.57%) in normal scenarios, while GL excels in convergence efficiency (1.1456s). After data poisoning, SGL shows superior resilience with an anomaly detection accuracy of 83.31%. The Hierarchical FedAvg and ADMM-based FL models exhibit lower communication and computational overhead, but experience significant accuracy drops during attacks. In addition, comparisons with existing techniques highlight a balance between accuracy, efficiency, and robustness, contributing to privacy-preserving anomaly detection systems for IoT networks.