Adaptive Aggregation Rules Enhancing Resilience in Federated Anomaly Detection for IoT

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 8 peer-reviewed papers addressing the following research question: Can adaptive aggregation rules in federated learning improve the resilience of unsupervised anomaly detection models against gradient poisoning in resource-constrained IoT environments. This work investigates the possibilities enabled by federated learning concerning IoT malware detection and studies security issues inherent to this new learning paradigm. In this context, a framework that uses federated learning to detect malware affecting IoT devices is. 12 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.7/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Federated Learning for Malware Detection in IoT Devices. Research question: Can adaptive aggregation rules in federated learning improve the resilience of unsupervised anomaly detection models against gradient poisoning in resource-constrained IoT environments?.

2 Methodology

Systematic literature search across multiple databases yielded 8 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.7/10.

3 Results

8 papers retrieved. 12 claims extracted; 0 independently verified. Quality review score: 3.7/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

5 Extracted Claims

Claim	Verified	Confidence
In Federated Learning (FL), algorithm training is performed in a decentralized manner by different nodes using local dat	×	0.09
In FL scenarios, each decentralized node trains an individual model using its own data and shares model parameters inste	×	0.05
The aggregation of model parameters to create a global model can be performed through a central server or a peer-to-peer	×	0.10
Previous works on FL for intrusion detection lack the use of realistic datasets in the FL context.	×	0.06
Previous works on FL for intrusion detection lack analysis on adversarial impact.	×	0.06
Previous works on FL for intrusion detection lack discussion of deployment in B5G scenarios.	×	0.06
The paper presents a use case involving a B5G scenario with Non-IID data and non-trusted stakeholders.	×	0.05
The proposed security framework covers both anomaly detection and classification approaches.	×	0.10
The dataset split described in Table (p6) includes a training set of 79%, a known test set of 20%, and 1% unused data.	×	0.03
An alternative dataset split described in Table (p6) allocates 39.5% for training, 39.5% for threshold selection, 20% fo	×	0.01
Table (p12) reports a centralized model performance metric of 95%.	×	0.06
Table (p12) contains data points indicating values of 7.8 and 7% associated with benign classifications.	×	0.03

References

- http://arxiv.org/abs/2104.09994v3
- http://arxiv.org/abs/2212.00966v1
- http://arxiv.org/abs/2409.13004v1