Supervised and Unsupervised Federated Learning for Cross-Device Malware Detection on N-BaIoT

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 7 peer-reviewed papers addressing the following research question: How does the performance of supervised versus unsupervised federated learning models compare on the N-BaIoT dataset using F1-score and AUC-ROC as evaluation metrics for cross-device malware detection. 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. 11 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.0/10. 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: How does the performance of supervised versus unsupervised federated learning models compare on the N-BaIoT dataset using F1-score and AUC-ROC as evaluation metrics for cross-device malware detection scenarios?.

2 Methodology

Systematic literature search across multiple databases yielded 7 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.0/10.

3 Results

7 papers retrieved. 11 claims extracted; 0 independently verified. Quality review score: 3.0/10.

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
Federated Learning (FL) is a collaborative machine learning paradigm where algorithm training is performed in a decentra	×	0.08
In Federated Learning, decentralized nodes share model parameters instead of raw data with other nodes or a central serv	×	0.06
The aggregation of model parameters in Federated Learning can be performed through a central entity (server) or via a pe	×	0.09
Previous works on Federated Learning for intrusion detection lack the use of realistic datasets in the FL context.	×	0.07
Previous works on Federated Learning for intrusion detection lack analysis on adversarial impact.	×	0.07
Previous works on Federated Learning for intrusion detection lack discussion of their deployment in B5G scenarios.	×	0.07
The paper presents a use case involving a B5G scenario with Non-IID (Independent and Identically Distributed) data and n	×	0.02
The proposed security framework covers both anomaly detection and classification approaches.	×	0.10
In the described data split, the training set comprises 79% of the data, the known test set comprises 20%, and 1% is unu	×	0.03
In an alternative data split configuration, the training set and threshold selection each comprise 39.5% of the data, wi	×	0.02
A centralized model configuration achieved a 95% performance metric in the reported results.	×	0.06

References

- http://arxiv.org/abs/2104.09994v3
- http://arxiv.org/abs/2305.11236v1
- http://arxiv.org/abs/2106.16020v1