Differential Privacy Noise Impact on F1-Score in Federated IoT Malware Detection

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 11 peer-reviewed papers addressing the following research question: What is the impact of differential privacy noise levels on the F1-score degradation of federated malware detection models when deployed on resource-constrained IoT devices. 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. 10 claims were extracted from source literature; 1 was independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 4.5/10. 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: What is the impact of differential privacy noise levels on the F1-score degradation of federated malware detection models when deployed on resource-constrained IoT devices?.

2 Methodology

Systematic literature search across multiple databases yielded 11 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 4.5/10.

3 Results

11 papers retrieved. 10 claims extracted; 1 independently verified. Quality review score: 4.5/10.

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 enables data privacy by design as data is not shared with any external identity.	×	0.10
Previous works dealing with FL for intrusion detection lack the use of realistic datasets in the FL context.	×	0.05
Previous works dealing with FL for intrusion detection lack the analysis on adversarial impact.	×	0.05
Previous works dealing with FL for intrusion detection lack the discussion of their deployment in B5G scenarios.	×	0.03
The proposed framework uses FL to detect cyberattacks affecting IoT devices in a privacy preserving fashion.	✓	0.17
The proposed framework covers both anomaly detection and classification approaches.	×	0.07
The benchmark table on page 5 shows model initialization, model aggregation, and server models.	×	0.07
The benchmark table on page 6 shows an aggregated updated global model with data preprocessing and model training.	×	0.07
The benchmark table on page 6 describes data splits including Train (79%), Unused (1%), and Known test (20%) for device	×	0.02
The benchmark table on page 12 shows 7.8% benign and 95% malicious data distribution in centralized scenarios.	×	0.03

References

- http://arxiv.org/abs/2209.14086v2

- http://arxiv.org/abs/2104.09994v3
- http://arxiv.org/abs/2207.02337v1