Federated Transfer Learning Generalization Across IoT Malware Datasets and Device Types

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 5 peer-reviewed papers addressing the following research question: How does federated transfer learning performance on N-BaIoT generalize to other IoT malware datasets when measured by cross-domain accuracy and F1 scores across different device types. 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. 7 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: How does federated transfer learning performance on N-BaIoT generalize to other IoT malware datasets when measured by cross-domain accuracy and F1 scores across different device types?.

2 Methodology

Systematic literature search across multiple databases yielded 5 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

5 papers retrieved. 7 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.	×	0.08
FL approaches can be used in the IoT context to build joint models without sharing sensitive data.	×	0.08
FL approaches affect the performance of traditional anomaly detectors and classifiers in IoT scenarios.	×	0.05
The proposed framework uses FL to detect cyberattacks affecting IoT devices in a privacy-preserving fashion.	✓	0.18
	×	0.00
The model achieves 95% benign detection rate in centralized testing (Table on p12).	×	0.05
The model achieves 7.8% benign detection rate for 50% of the devices (Table on p12).	×	0.07

References

- http://arxiv.org/abs/2104.09994v3
- http://arxiv.org/abs/2209.05395v1
- http://arxiv.org/abs/2007.06081v1