Federated Transfer Learning for Cross-Domain Malware Detection in IoT Devices

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 6 peer-reviewed papers addressing the following research question: To what extent does domain adaptation via federated transfer learning improve model generalization in malware detection when trained on N-BaIoT and evaluated on unseen IoT device types, measured by. 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. 5 claims were extracted from source literature; 1 was independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 4.8/10. 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: To what extent does domain adaptation via federated transfer learning improve model generalization in malware detection when trained on N-BaIoT and evaluated on unseen IoT device types, measured by precision-recall curves on cross-domain test sets?.

2 Methodology

Systematic literature search across multiple databases yielded 6 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 4.8/10.

3 Results

6 papers retrieved. 5 claims extracted; 1 independently verified. Quality review score: 4.8/10.

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.	×	0.07
Previous works dealing with FL for intrusion detection lack the use of realistic datasets in the FL context.	×	0.05
The proposed framework covers both anomaly detection and classification approaches using multi-model techniques.	×	0.09
The security framework uses FL to detect cyber-attacks affecting IoT devices in a privacy preserving fashion.	✓	0.18
The model achieves 95% accuracy in centralized learning scenarios.	×	0.05

References

- http://arxiv.org/abs/2104.09994v3
- http://arxiv.org/abs/1902.02401v1
- http://arxiv.org/abs/2207.02337v1