Federated Learning Aggregation Strategies for Heterogeneous IoT Malware Detection Performance

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 8 peer-reviewed papers addressing the following research question: What is the impact of different federated learning aggregation strategies (e.g., FedAvg, FedProx) on malware detection performance across heterogeneous IoT device types when measured by. In this paper, we investigate Federated Learning (FL), a paradigm of machine learning that allows for decentralized model training on devices without sharing raw data, there by preserving data privacy. In particular, we compare two strategies within this paradigm: Federated. 12 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.1/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: A Comparative Evaluation of FedAvg and Per-FedAvg Algorithms for Dirichlet Distributed Heterogeneous Data. Research question: What is the impact of different federated learning aggregation strategies (e.g., FedAvg, FedProx) on malware detection performance across heterogeneous IoT device types when measured by precision-recall curves?.

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 3.1/10.

3 Results

8 papers retrieved. 12 claims extracted; 0 independently verified. Quality review score: 3.1/10.

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 Averaging (FedAvg) was introduced by McMahan et al.	×	0.07
FedAvg combines local updates computed through stochastic gradient descent (SGD) on each client with a server that perfo	×	0.11
FedAvg is effective in scenarios where data is unbalanced and non-IID.	×	0.11
FedAvg can significantly reduce the rounds of communication needed to train a deep network on decentralized data.	×	0.05
Under parameters α = 0.5 and τ = 10, FedAvg achieved an accuracy of 53.24%.	×	0.02
Under parameters α = 0.5 and τ = 4, FedAvg achieved an accuracy of 38.31%.	×	0.02
Under parameters α = 0.1 and τ = 10, FedAvg achieved an accuracy of 59.42%.	×	0.02
Under parameters α = 0.1 and τ = 4, FedAvg achieved an accuracy of 53.20%.	×	0.02
Under parameters α = 0.5 and τ = 10, Per-FedAvg achieved an accuracy of 79.73%.	×	0.02
Under parameters α = 0.5 and τ = 4, Per-FedAvg achieved an accuracy of 72.07%.	×	0.02
Secure aggregation protocols for privacy-preserving machine learning are communication-efficient and failure-robust.	×	0.09
Potential security threats in Federated Learning include data poisoning and adversarial attacks.	×	0.04

References

- http://arxiv.org/abs/2007.05690v4
- http://arxiv.org/abs/2309.01275v1
- http://arxiv.org/abs/2406.07800v2