

Scaling Federated Clients in Lightweight Malware Detection on Edge Devices

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 9 peer-reviewed papers addressing the following research question: How does increasing the number of federated clients impact the inference latency and throughput of lightweight malware detection models on edge devices when evaluated on the N-BaIoT dataset. In this paper, we propose a new comprehensive realistic cyber security dataset of IoT and IIoT applications, called Edge-IIoTset, which can be used by machine learning-based intrusion detection systems in two different modes, namely, centralized and federated learning. 11 claims were extracted from source literature; 6 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 6.7/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. Research question: How does increasing the number of federated clients impact the inference latency and throughput of lightweight malware detection models on edge devices when evaluated on the N-BaIoT dataset?.

2 Methodology

Systematic literature search across multiple databases yielded 9 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 6.7/10.

3 Results

9 papers retrieved. 11 claims extracted; 6 independently verified. Quality review score: 6.7/10.

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
The Edge-IIoTset dataset is designed for use in both centralized and federated learning modes.	✓	0.19
The Edge-IIoTset dataset was generated using a purpose-built IoT/IIoT testbed.	✓	0.28
The testbed used to generate Edge-IIoTset includes more than 10 types of IoT devices.	×	0.12
Specific devices used in the testbed include Low-cost digital sensors for temperature and humidity, Ultrasonic sensor, W	✓	0.35
The dataset identifies and analyzes fourteen attacks related to IoT and IIoT connectivity protocols.	✓	0.21
The fourteen identified attacks are categorized into five threat types: DoS/DDoS attacks, Information gathering, Man in	✓	0.22
Features in the dataset were extracted from alerts, system resources, logs, and network traffic.	×	0.14
A total of 1176 features were initially found in the dataset.	×	0.06
61 new features with high correlations were proposed and selected from the initial 1176 features.	×	0.12
The paper evaluates the performance of traditional machine learning and deep learning approaches on the Edge-IIoTset dat	✓	0.19
The evaluation covers both centralized and federated learning modes.	×	0.15

References

- <https://doi.org/10.1109/access.2022.3165809>
- <https://doi.org/10.1109/access.2020.2991734>
- <https://doi.org/10.1109/access.2021.3118642>