Differential Privacy Trade-offs in Federated Malware Detection on N-BaIoT

Assignee Research

May 30, 2026

Abstract

This report synthesises findings from 14 peer-reviewed papers addressing the following research question: What is the impact of differential privacy techniques on the trade-off between malware detection accuracy and bandwidth utilization in federated learning models trained on the N-BaIoT dataset. In this article, we present a comprehensive study with an experimental analysis of federated deep learning approaches for cyber security in the Internet of Things (IoT) applications. Specifically, we first provide a review of the federated learning-based security and privacy. 7 claims were extracted from source literature; 7 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.2/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis. Research question: What is the impact of differential privacy techniques on the trade-off between malware detection accuracy and bandwidth utilization in federated learning models trained on the N-BaIoT dataset?.

2 Methodology

Systematic literature search across multiple databases yielded 14 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.2/10.

3 Results

14 papers retrieved. 7 claims extracted; 7 independently verified. Quality review score: 7.2/10.

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 study reviews federated learning-based security and privacy systems for Industrial IoT, Edge Computing, Internet of	✓	0.33
The article discusses the integration of federated learning with blockchain and malware/intrusion detection systems for	✓	0.23
The study reviews vulnerabilities present in federated learning-based security and privacy systems.	✓	0.19
The experimental analysis utilizes three deep learning approaches: Recurrent Neural Network (RNN), Convolutional Neural	✓	0.37
The performance of centralized and federated learning was studied for each deep learning model using the Bot-IoT, MQTTse	✓	0.18
Federated deep learning approaches outperform classic/centralized machine learning versions in assuring the privacy of I	✓	0.32
Federated deep learning approaches provide higher accuracy in detecting attacks compared to classic/centralized machine	✓	0.28

References

- https://doi.org/10.3390/jsan14040078
- https://doi.org/10.1007/s10462-024-11082-w

- https://doi.org/10.1109/access.2021.3118642