# Asynchronous Client Participation and Poisoning Robustness in Federated IoT Malware Detection

Assignee Research

May 31, 2026

**Abstract**

This report synthesises findings from 14 peer-reviewed papers addressing the following research question: What is the effect of asynchronous client participation rates on the robustness of federated learning algorithms against poisoning attacks in IoT malware detection scenarios. 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; 6 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.3/10. 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 effect of asynchronous client participation rates on the robustness of federated learning algorithms against poisoning attacks in IoT malware detection scenarios?.

## 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 7.3/10.

## 3 Results

14 papers retrieved. 7 claims extracted; 6 independently verified. Quality review score: 7.3/10.

## 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 | ✓ | 0.34 |
| The article discusses the integration of federated learning with blockchain and malware/intrusion detection systems for | ✓ | 0.23 |
| The study reviews vulnerabilities in federated learning-based security and privacy systems. | ✓ | 0.23 |
| The experimental analysis utilizes three deep learning approaches: Recurrent Neural Network (RNN), Convolutional Neural | ✓ | 0.39 |
| The performance of centralized and federated learning was studied using the Bot-IoT, MQTTset, and TON_IoT datasets. | × | 0.15 |
| Federated deep learning approaches outperform classic/centralized machine learning versions in assuring the privacy of I | ✓ | 0.33 |
| Federated deep learning approaches provide higher accuracy in detecting attacks compared to classic/centralized machine | ✓ | 0.29 |

## References


- https://doi.org/10.3390/app8122663
- https://doi.org/10.63125/ry033286

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