

# Federated Intrusion Detection Robustness Under Non-IID IoT Data Distributions

Assignee Research

May 31, 2026

## Abstract

This report synthesises findings from 16 peer-reviewed papers addressing the following research question: What is the impact of non-IID data distributions across different IoT device types on the robustness and false positive rates of federated intrusion detection models compared to centralized training. 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. 10 claims were extracted from source literature; 6 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 7.0/10. 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 non-IID data distributions across different IoT device types on the robustness and false positive rates of federated intrusion detection models compared to centralized training?.

## 2 Methodology

Systematic literature search across multiple databases yielded 16 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 7.0/10.

### 3 Results

16 papers retrieved. 10 claims extracted; 6 independently verified. Quality review score: 7.0/10.

### 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 in federated learning-based security and privacy systems.	✓	0.23
The experimental analysis utilizes three deep learning approaches: Recurrent Neural Network (RNN), Convolutional Neural	✓	0.38
The study compares the performance of centralized and federated learning models.	×	0.12
The experiments were conducted using the Bot-IoT dataset.	×	0.10
The experiments were conducted using the MQTTset dataset.	×	0.07
The experiments were conducted using the TON_IoT dataset.	×	0.07
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	✓	0.28

## References

- <https://doi.org/10.3390/app8122663>
- <https://doi.org/10.1145/3448300.3467827>
- <https://doi.org/10.1109/access.2021.3118642>