Federated Learning Aggregation Rules and Their Impact on Edge-Based Intrusion Detection Efficiency

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 12 peer-reviewed papers addressing the following research question: How do different aggregation rules in federated learning affect the inference efficiency and detection latency of deep learning-based intrusion detection systems on edge devices. Intrusion detection systems are evolving into intelligent systems that perform data analysis searching for anomalies in their environment. The development of deep learning technologies opened the door to build more complex and effective threat detection models. 13 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.0/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: A review of Federated Learning in Intrusion Detection Systems for IoT. Research question: How do different aggregation rules in federated learning affect the inference efficiency and detection latency of deep learning-based intrusion detection systems on edge devices?.

2 Methodology

Systematic literature search across multiple databases yielded 12 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.0/10.

3 Results

12 papers retrieved. 13 claims extracted; 0 independently verified. Quality review score: 3.0/10.

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 warm-up strategy for Non-IID data involves randomly selecting k nodes to share 5%-10% of their dataset with the serv	×	0.08
Sharing a small proportion (5%-10%) of datasets in the warm-up strategy mitigates the impact of violating Federated Lear	×	0.06
Scenario S1 is defined as the absence of false negatives and the absence of false positives.	×	0.03
Scenario S4 represents the worst case, characterized by only false negatives and only false positives.	×	0.02
In Scenario S3, the PR curve shows a greater distance from the default baseline than the ROC curve shows from the random	×	0.03
The PR curve does not consider true negatives.	×	0.02
NIDS focus on network traffic to find malicious patterns targeting devices inside a monitored infrastructure.	×	0.04
Leveraging ML techniques for intrusion detection is a successful methodology for learning complex relationships in data	×	0.09
Molina et al. established that input data types for NIDS include raw traffic, data flows, and encrypted payloads.	×	0.02
Molina et al. established that input data types for HIDS include application data, memory accesses, and kernel operation	×	0.03
Misuse-based detectors identify potential threats by relying on attack signatures, patterns, or rules.	×	0.02
Anomaly-based detectors operate by detecting abnormal patterns that deviate from expected observations or common behavio	×	0.03
Hybrid detectors combine misuse and anomaly-based detectors to create more robust systems.	×	0.05

References

- `http://arxiv.org/abs/1910.08635v2`

- http://arxiv.org/abs/2502.06963v3
- http://arxiv.org/abs/2204.12443v2