Scaling Effects on Federated Learning Robustness Against Adversarial Poisoning in IoT

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 10 peer-reviewed papers addressing the following research question: How does model scaling affect the robustness of federated learning systems against adversarial poisoning attacks in IoT security applications. Due to its distributed nature, federated learning is vulnerable to poisoning attacks, in which malicious clients poison the training process via manipulating their local training data and/or local model updates sent to the cloud server, such that the poisoned global model. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.7/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: FLCert: Provably Secure Federated Learning against Poisoning Attacks. Research question: How does model scaling affect the robustness of federated learning systems against adversarial poisoning attacks in IoT security applications?.

2 Methodology

Systematic literature search across multiple databases yielded 10 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.7/10.

3 Results

10 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 3.7/10.

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.

References

- http://arxiv.org/abs/2104.09994v3
- http://arxiv.org/abs/2310.11594v3
- http://arxiv.org/abs/2210.00584v2