Defense-Free vs. Byzantine-Robust Federated Learning on CIFAR-10 Under Label-Flipping Attacks

Assignee Research

May 31, 2026

Abstract

This report synthesises findings from 10 peer-reviewed papers addressing the following research question: How do defense-free federated learning frameworks compare to Byzantine-robust aggregators like Krum or Median in terms of test accuracy on CIFAR-10 under 20% and 40% label-flipping poisoning rates. Federated learning (FL) allows multiple clients to collaboratively train a global machine learning model through a server, without exchanging their private training data. However, the decentralized aspect of FL makes it susceptible to poisoning attacks, where malicious clients. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 6.0/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Do We Really Need to Design New Byzantine-robust Aggregation Rules?. Research question: How do defense-free federated learning frameworks compare to Byzantine-robust aggregators like Krum or Median in terms of test accuracy on CIFAR-10 under 20% and 40% label-flipping poisoning rates?.

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 6.0/10.

3 Results

10 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 6.0/10.

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.

References

- http://arxiv.org/abs/2406.12222v1
- http://arxiv.org/abs/2501.17381v1
- http://arxiv.org/abs/2310.04414v3