# Random Layer Aggregation Effects on Inference Efficiency and Attack Resilience in Federated Learning

Assignee Research

May 31, 2026

**Abstract**

This report synthesises findings from 11 peer-reviewed papers addressing the following research question: What is the impact of random layer aggregation on inference efficiency and attack resilience in resource-constrained federated learning models. Federated Learning (FL) is increasingly applied in sectors like healthcare, finance, and IoT, enabling collaborative model training while safeguarding user privacy. However, FL systems are susceptible to Byzantine adversaries that inject malicious updates, which can severely. 17 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.2/10. This report is a machine-generated literature synthesis and does not constitute original research.

## 1 Introduction

This paper examines: Dynamic Meta-Layer Aggregation for Byzantine-Robust Federated Learning. Research question: What is the impact of random layer aggregation on inference efficiency and attack resilience in resource-constrained federated learning models?.

## 2 Methodology

Systematic literature search across multiple databases yielded 11 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.2/10.

## 3 Results

11 papers retrieved. 17 claims extracted; 0 independently verified. Quality review score: 3.2/10.

## 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 |
|---|---|---|
| FedAOT was evaluated on benchmark datasets using a federated learning simulation with 20 to 100 clients. | × | 0.07 |
| Byzantine clients ranged from 20% to 90% of the total population in the experiments. | × | 0.03 |
| Each client trained a CNN and FNN hybrid model locally using the Adam optimizer with a learning rate of 0.001 and a batc | × | 0.04 |
| Experiments were conducted in a Linux-based environment (Kaggle Notebooks) equipped with two NVIDIA T4 GPUs. | × | 0.02 |
| Federated simulations were implemented using the Flower framework with PyTorch. | × | 0.03 |
| In the label-flipping scenario, malicious clients modify the entire label set using the rule (label + 1) mod 10. | × | 0.10 |
| FedAOT was compared with FedAvg, FoolsGold, and GeoMed aggregation methods. | × | 0.08 |
| Performance was evaluated on the test set using classification accuracy and F1 score. | × | 0.05 |
| The proposed method was evaluated using MNIST, KMNIST, and FashionMNIST datasets. | × | 0.05 |
| On the MNIST dataset under A20 attack intensity, FedAOT achieved classification accuracies of 98.78% and 98.77% across r | × | 0.04 |
| On the MNIST dataset under A90 attack intensity, FedAOT achieved classification accuracies of 97.77% and 97.75% across r | × | 0.02 |
| On the KMNIST dataset under A20 attack intensity, FedAOT achieved classification accuracies of 94.84% and 94.83% across | × | 0.02 |
| On the KMNIST dataset under A90 attack intensity, FedAOT achieved classification accuracies of 91.66% and 91.64% across | × | 0.03 |
| On the FashionMNIST dataset under A20 attack intensity, FedAOT achieved classification accuracies of 89.53% and 89.54% a | × | 0.02 |
| On the FashionMNIST dataset under A90 attack intensity, FedAOT achieved classification accuracies of 88.46% and 88.44% a | × | 0.02 |
| FedAOT accuracy remains consistently high even when up to 90% of the participating clients are malicious. | × | 0.04 |
| Traditional aggregation schemes often fail to converge under adversarial influence where malicious clients inject random | × | 0.08 |

## References


- https://arxiv.org/abs/2603.16846
- http://arxiv.org/abs/2206.02535v2
- https://www.semanticscholar.org/paper/631f733ae355e2535785080aa27aa106f314742f