FL Simulation Results

File: test1_pyth

Federated Learning Configuration

Total Clients (N): 5

Malicious Clients (M): 3

Neural Network: MyNN

Training Rounds: 5

Poisoned Rounds (R): 3

Distribution Strategy: first

Data Poisoning Attack Parameters

Poisoning Operation: Label Flip

Attack Intensity: 10.0% (0.10)

Poisoned Data Percentage: 20.0% (0.20)

Attack Summary: Using label_flip with 10.0% (0.10) intensity on 20.0% (0.20) of data for 3 rounds with 3 malicious clients.

Simulation Results

Init Accuracy: 0.8807

Clean Accuracy: 0.6568

Poisoned Accuracy: 0.2220

Poisoned + DP Protection Accuracy: 0.1357

Drop (Clean - Poisoned): 0.4348

Drop (Clean - Init): -0.2239

Drop (Poisoned - Init): -0.6587

Drop (Poisoned DP - Init): -0.7450

DP Protection Method: krum

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.7458

Clean Recall: 0.6568

Clean F1 Score: 0.6474

Poisoned Precision: 0.7786

Poisoned Recall: 0.2051

Poisoned F1 Score: 0.1910

DP Protection Precision: 0.3357

DP Protection Recall: 0.1149

DP Protection F1 Score: 0.0497

Summary

FL Simulation Complete
Task: c91b37a5-25bd-4df7-a54e-048ddc6768af
GPU: GPU 2
Init Accuracy: 0.8807
Clean Accuracy: 0.6568
Poisoned Accuracy: 0.2220
Data Poison Protection Accuracy: 0.1357
Drop (Clean - Poisoned): 0.4348
Drop (Clean - Init): -0.2239
Drop (Poisoned - Init): -0.6587
Drop (Poisoned_DP - Init): -0.7450
Data Poison Protection Method: krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.7458
Clean Recall: 0.6568
Clean F1 Score: 0.6474
Poisoned Precision: 0.7786
Poisoned Recall: 0.2051
Poisoned F1 Score: 0.1910
DP Protection Precision: 0.3357
DP Protection Recall: 0.1149
DP Protection F1 Score: 0.0497