FL Simulation Results

File: sim_LabelFlip_3_Trimmed

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 3

Neural Network: Test1.1_

Training Rounds: 5

Poisoned Rounds (R): 5

Distribution Strategy: first

Data Poisoning Attack Parameters

Poisoning Operation: Label Flip

Attack Intensity: 15.0% (0.15)

Poisoned Data Percentage: 30.0% (0.30)

Attack Summary: Using label_flip with 15.0% (0.15) intensity on 30.0% (0.30) of data for 5 rounds with 3 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9471

Clean + DP Protection Accuracy: 0.9454

Poisoned Accuracy: 0.9427

Poisoned + DP Protection Accuracy: 0.9389

Drop (Clean - Poisoned): 0.0044

Drop (Clean - Init): 0.0026

Drop (Clean DP - Init): 0.0009

Drop (Poisoned - Init): -0.0018

Drop (Poisoned DP - Init): -0.0056

DP Protection Method: trimmed_mean

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9470

Clean Recall: 0.9471

Clean F1 Score: 0.9469

Clean DP Precision: 0.9453

Clean DP Recall: 0.9454

Clean DP F1 Score: 0.9453

Poisoned Precision: 0.9429

Poisoned Recall: 0.9427

Poisoned F1 Score: 0.9426

DP Protection Precision: 0.9397

DP Protection Recall: 0.9389

DP Protection F1 Score: 0.9389

Summary

FL Simulation Complete
Task: 844d3aed-e409-453d-a3d9-2edddb707a6b
GPU: GPU 2
Init Accuracy: 0.9445
Clean Accuracy: 0.9471
Clean DP Accuracy: 0.9454
Poisoned Accuracy: 0.9427
Data Poison Protection Accuracy: 0.9389
Drop (Clean - Poisoned): 0.0044
Drop (Clean - Init): 0.0026
Drop (Clean DP - Init): 0.0009
Drop (Poisoned - Init): -0.0018
Drop (Poisoned_DP - Init): -0.0056
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9470
Clean Recall: 0.9471
Clean F1 Score: 0.9469
Clean DP Precision: 0.9453
Clean DP Recall: 0.9454
Clean DP F1 Score: 0.9453
Poisoned Precision: 0.9429
Poisoned Recall: 0.9427
Poisoned F1 Score: 0.9426
DP Protection Precision: 0.9397
DP Protection Recall: 0.9389
DP Protection F1 Score: 0.9389