FL Simulation Results

File: test1_LabelFlip_5_Trimmed

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 5

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 5 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9470

Clean + DP Protection Accuracy: 0.9460

Poisoned Accuracy: 0.9486

Poisoned + DP Protection Accuracy: 0.9487

Drop (Clean - Poisoned): -0.0016

Drop (Clean - Init): 0.0025

Drop (Clean DP - Init): 0.0015

Drop (Poisoned - Init): 0.0041

Drop (Poisoned DP - Init): 0.0042

DP Protection Method: trimmed_mean

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9470

Clean Recall: 0.9470

Clean F1 Score: 0.9469

Clean DP Precision: 0.9459

Clean DP Recall: 0.9460

Clean DP F1 Score: 0.9458

Poisoned Precision: 0.9487

Poisoned Recall: 0.9486

Poisoned F1 Score: 0.9486

DP Protection Precision: 0.9487

DP Protection Recall: 0.9487

DP Protection F1 Score: 0.9486

Summary

FL Simulation Complete
Task: 2baebba0-9970-4386-a4fb-c02efb56a562
GPU: GPU 2
Init Accuracy: 0.9445
Clean Accuracy: 0.9470
Clean DP Accuracy: 0.9460
Poisoned Accuracy: 0.9486
Data Poison Protection Accuracy: 0.9487
Drop (Clean - Poisoned): -0.0016
Drop (Clean - Init): 0.0025
Drop (Clean DP - Init): 0.0015
Drop (Poisoned - Init): 0.0041
Drop (Poisoned_DP - Init): 0.0042
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9470
Clean Recall: 0.9470
Clean F1 Score: 0.9469
Clean DP Precision: 0.9459
Clean DP Recall: 0.9460
Clean DP F1 Score: 0.9458
Poisoned Precision: 0.9487
Poisoned Recall: 0.9486
Poisoned F1 Score: 0.9486
DP Protection Precision: 0.9487
DP Protection Recall: 0.9487
DP Protection F1 Score: 0.9486