FL Simulation Results

File: test1.2

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 3

Neural Network: MyNN

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: 0.9274

Poisoned Accuracy: 0.5966

Poisoned + DP Protection Accuracy: 0.6712

Drop (Clean - Poisoned): 0.3308

Drop (Clean - Init): -0.0171

Drop (Poisoned - Init): -0.3479

Drop (Poisoned DP - Init): -0.2733

DP Protection Method: fedavg

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9289

Clean Recall: 0.9274

Clean F1 Score: 0.9268

Poisoned Precision: 0.7923

Poisoned Recall: 0.6010

Poisoned F1 Score: 0.6560

DP Protection Precision: 0.7862

DP Protection Recall: 0.6858

DP Protection F1 Score: 0.7240

Summary

FL Simulation Complete
Task: d8a189ef-b9af-4f8e-9020-88a03ba843cc
GPU: GPU 2
Init Accuracy: 0.9445
Clean Accuracy: 0.9274
Poisoned Accuracy: 0.5966
Data Poison Protection Accuracy: 0.6712
Drop (Clean - Poisoned): 0.3308
Drop (Clean - Init): -0.0171
Drop (Poisoned - Init): -0.3479
Drop (Poisoned_DP - Init): -0.2733
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9289
Clean Recall: 0.9274
Clean F1 Score: 0.9268
Poisoned Precision: 0.7923
Poisoned Recall: 0.6010
Poisoned F1 Score: 0.6560
DP Protection Precision: 0.7862
DP Protection Recall: 0.6858
DP Protection F1 Score: 0.7240