FL Simulation Results

File: test1.1

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 1

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 1 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9230

Poisoned Accuracy: 0.6942

Poisoned + DP Protection Accuracy: 0.6959

Drop (Clean - Poisoned): 0.2288

Drop (Clean - Init): -0.0215

Drop (Poisoned - Init): -0.2503

Drop (Poisoned DP - Init): -0.2486

DP Protection Method: fedavg

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9269

Clean Recall: 0.9230

Clean F1 Score: 0.9234

Poisoned Precision: 0.7582

Poisoned Recall: 0.7131

Poisoned F1 Score: 0.7227

DP Protection Precision: 0.7648

DP Protection Recall: 0.7132

DP Protection F1 Score: 0.7298

Summary

FL Simulation Complete
Task: d595f2b3-0d52-4984-87a1-bb6ffcc3157b
GPU: GPU 2
Init Accuracy: 0.9445
Clean Accuracy: 0.9230
Poisoned Accuracy: 0.6942
Data Poison Protection Accuracy: 0.6959
Drop (Clean - Poisoned): 0.2288
Drop (Clean - Init): -0.0215
Drop (Poisoned - Init): -0.2503
Drop (Poisoned_DP - Init): -0.2486
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9269
Clean Recall: 0.9230
Clean F1 Score: 0.9234
Poisoned Precision: 0.7582
Poisoned Recall: 0.7131
Poisoned F1 Score: 0.7227
DP Protection Precision: 0.7648
DP Protection Recall: 0.7132
DP Protection F1 Score: 0.7298