FL Simulation Results

File: test1.1_FedAvg

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 1

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 1 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9289

Poisoned Accuracy: 0.6177

Poisoned + DP Protection Accuracy: 0.5659

Drop (Clean - Poisoned): 0.3112

Drop (Clean - Init): -0.0156

Drop (Poisoned - Init): -0.3268

Drop (Poisoned DP - Init): -0.3786

DP Protection Method: fedavg

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9313

Clean Recall: 0.9289

Clean F1 Score: 0.9288

Poisoned Precision: 0.7712

Poisoned Recall: 0.6254

Poisoned F1 Score: 0.6690

DP Protection Precision: 0.7761

DP Protection Recall: 0.5682

DP Protection F1 Score: 0.6215

Summary

FL Simulation Complete
Task: 4b5c4d81-258b-4b6f-8341-936e9a722fdd
GPU: GPU 0
Init Accuracy: 0.9445
Clean Accuracy: 0.9289
Poisoned Accuracy: 0.6177
Data Poison Protection Accuracy: 0.5659
Drop (Clean - Poisoned): 0.3112
Drop (Clean - Init): -0.0156
Drop (Poisoned - Init): -0.3268
Drop (Poisoned_DP - Init): -0.3786
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9313
Clean Recall: 0.9289
Clean F1 Score: 0.9288
Poisoned Precision: 0.7712
Poisoned Recall: 0.6254
Poisoned F1 Score: 0.6690
DP Protection Precision: 0.7761
DP Protection Recall: 0.5682
DP Protection F1 Score: 0.6215