FL Simulation Results

File: test1.1_tf_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: 0.7334

Clean Accuracy: 0.8661

Poisoned Accuracy: 0.7141

Poisoned + DP Protection Accuracy: 0.7196

Drop (Clean - Poisoned): 0.1520

Drop (Clean - Init): 0.1327

Drop (Poisoned - Init): -0.0193

Drop (Poisoned DP - Init): -0.0138

DP Protection Method: fedavg

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.8660

Clean Recall: 0.8661

Clean F1 Score: 0.8653

Poisoned Precision: 0.6973

Poisoned Recall: 0.7391

Poisoned F1 Score: 0.7107

DP Protection Precision: 0.6995

DP Protection Recall: 0.7460

DP Protection F1 Score: 0.7141

Summary

FL Simulation Complete
Task: c0318598-0e25-4e7b-b9b5-49636f134b7f
GPU: GPU 2
Init Accuracy: 0.7334
Clean Accuracy: 0.8661
Poisoned Accuracy: 0.7141
Data Poison Protection Accuracy: 0.7196
Drop (Clean - Poisoned): 0.1520
Drop (Clean - Init): 0.1327
Drop (Poisoned - Init): -0.0193
Drop (Poisoned_DP - Init): -0.0138
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.8660
Clean Recall: 0.8661
Clean F1 Score: 0.8653
Poisoned Precision: 0.6973
Poisoned Recall: 0.7391
Poisoned F1 Score: 0.7107
DP Protection Precision: 0.6995
DP Protection Recall: 0.7460
DP Protection F1 Score: 0.7141