FL Simulation Results

File: test2.1

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 3

Neural Network: MyNN

Training Rounds: 5

Poisoned Rounds (R): 3

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 3 rounds with 3 malicious clients.

Simulation Results

Init Accuracy: 0.7334

Clean Accuracy: 0.8560

Poisoned Accuracy: 0.6099

Poisoned + DP Protection Accuracy: 0.5993

Drop (Clean - Poisoned): 0.2461

Drop (Clean - Init): 0.1226

Drop (Poisoned - Init): -0.1235

Drop (Poisoned DP - Init): -0.1341

DP Protection Method: fedavg

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.8589

Clean Recall: 0.8560

Clean F1 Score: 0.8558

Poisoned Precision: 0.7040

Poisoned Recall: 0.6168

Poisoned F1 Score: 0.6232

DP Protection Precision: 0.7128

DP Protection Recall: 0.6037

DP Protection F1 Score: 0.6164

Summary

FL Simulation Complete
Task: beb71d59-b6e8-4ae9-9649-10f5b4cbe327
GPU: GPU 2
Init Accuracy: 0.7334
Clean Accuracy: 0.8560
Poisoned Accuracy: 0.6099
Data Poison Protection Accuracy: 0.5993
Drop (Clean - Poisoned): 0.2461
Drop (Clean - Init): 0.1226
Drop (Poisoned - Init): -0.1235
Drop (Poisoned_DP - Init): -0.1341
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.8589
Clean Recall: 0.8560
Clean F1 Score: 0.8558
Poisoned Precision: 0.7040
Poisoned Recall: 0.6168
Poisoned F1 Score: 0.6232
DP Protection Precision: 0.7128
DP Protection Recall: 0.6037
DP Protection F1 Score: 0.6164