FL Simulation Results

File: test1.1_New_Net_

Federated Learning Configuration

Total Clients (N): 2

Malicious Clients (M): 1

Neural Network: MyNN

Training Rounds: 2

Poisoned Rounds (R): 1

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 1 rounds with 1 malicious clients.

Simulation Results

Init Accuracy: 0.1010

Clean Accuracy: 0.9270

Poisoned Accuracy: 0.1701

Poisoned + DP Protection Accuracy: 0.1431

Drop (Clean - Poisoned): 0.7569

Drop (Clean - Init): 0.8260

Drop (Poisoned - Init): 0.0691

Drop (Poisoned DP - Init): 0.0421

DP Protection Method: fedavg

GPU Used: GPU 1

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9415

Clean Recall: 0.9282

Clean F1 Score: 0.9276

Poisoned Precision: 0.2009

Poisoned Recall: 0.1273

Poisoned F1 Score: 0.0752

DP Protection Precision: 0.1143

DP Protection Recall: 0.1004

DP Protection F1 Score: 0.0259

Summary

FL Simulation Complete
Task: 64290d44-cc29-45ff-899e-e5bc7e5afafd
GPU: GPU 1
Init Accuracy: 0.1010
Clean Accuracy: 0.9270
Poisoned Accuracy: 0.1701
Data Poison Protection Accuracy: 0.1431
Drop (Clean - Poisoned): 0.7569
Drop (Clean - Init): 0.8260
Drop (Poisoned - Init): 0.0691
Drop (Poisoned_DP - Init): 0.0421
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9415
Clean Recall: 0.9282
Clean F1 Score: 0.9276
Poisoned Precision: 0.2009
Poisoned Recall: 0.1273
Poisoned F1 Score: 0.0752
DP Protection Precision: 0.1143
DP Protection Recall: 0.1004
DP Protection F1 Score: 0.0259