FL Simulation Results

File: test1.1___

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: 0.9318

Poisoned Accuracy: 0.7464

Poisoned + DP Protection Accuracy: 0.7240

Drop (Clean - Poisoned): 0.1854

Drop (Clean - Init): -0.0127

Drop (Poisoned - Init): -0.1981

Drop (Poisoned DP - Init): -0.2205

DP Protection Method: trimmed_mean_krum

GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9333

Clean Recall: 0.9318

Clean F1 Score: 0.9314

Poisoned Precision: 0.7509

Poisoned Recall: 0.7722

Poisoned F1 Score: 0.7548

DP Protection Precision: 0.7472

DP Protection Recall: 0.7473

DP Protection F1 Score: 0.7367

Summary

FL Simulation Complete
Task: bd72e410-49e5-4fc2-8b3a-1467d7d7ea8a
GPU: GPU 2
Init Accuracy: 0.9445
Clean Accuracy: 0.9318
Poisoned Accuracy: 0.7464
Data Poison Protection Accuracy: 0.7240
Drop (Clean - Poisoned): 0.1854
Drop (Clean - Init): -0.0127
Drop (Poisoned - Init): -0.1981
Drop (Poisoned_DP - Init): -0.2205
Data Poison Protection Method: trimmed_mean_krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9333
Clean Recall: 0.9318
Clean F1 Score: 0.9314
Poisoned Precision: 0.7509
Poisoned Recall: 0.7722
Poisoned F1 Score: 0.7548
DP Protection Precision: 0.7472
DP Protection Recall: 0.7473
DP Protection F1 Score: 0.7367