FL Simulation Results

File: test1.2

Federated Learning Configuration

Total Clients (N): 10

Malicious Clients (M): 3

Neural Network: Test1.2_

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 3 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9306

Poisoned Accuracy: 0.6318

Poisoned + DP Protection Accuracy: 0.5932

Drop (Clean - Poisoned): 0.2988

Drop (Clean - Init): -0.0139

Drop (Poisoned - Init): -0.3127

Drop (Poisoned DP - Init): -0.3513

DP Protection Method: trimmed_mean

GPU Used: GPU 1

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9337

Clean Recall: 0.9306

Clean F1 Score: 0.9310

Poisoned Precision: 0.7671

Poisoned Recall: 0.6439

Poisoned F1 Score: 0.6572

DP Protection Precision: 0.7607

DP Protection Recall: 0.5994

DP Protection F1 Score: 0.6236

Summary

FL Simulation Complete
Task: 228fde96-cf25-47e4-b49c-ccb1ebcd233e
GPU: GPU 1
Init Accuracy: 0.9445
Clean Accuracy: 0.9306
Poisoned Accuracy: 0.6318
Data Poison Protection Accuracy: 0.5932
Drop (Clean - Poisoned): 0.2988
Drop (Clean - Init): -0.0139
Drop (Poisoned - Init): -0.3127
Drop (Poisoned_DP - Init): -0.3513
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9337
Clean Recall: 0.9306
Clean F1 Score: 0.9310
Poisoned Precision: 0.7671
Poisoned Recall: 0.6439
Poisoned F1 Score: 0.6572
DP Protection Precision: 0.7607
DP Protection Recall: 0.5994
DP Protection F1 Score: 0.6236