FL Simulation Results

File: sig_backdoor_trimmed_more_Clients

Federated Learning Configuration

Total Clients (N): 5

Malicious Clients (M): 1

Neural Network: Test1.1_

Training Rounds: 2

Poisoned Rounds (R): 1

Distribution Strategy: first

Data Poisoning Attack Parameters

Poisoning Operation: backdoor_sig

Attack Intensity: 15.0% (0.15)

Poisoned Data Percentage: 30.0% (0.30)

Attack Summary: Using backdoor_sig with 15.0% (0.15) intensity on 30.0% (0.30) of data for 1 rounds with 1 malicious clients.

Simulation Results

Init Accuracy: 0.9445

Clean Accuracy: 0.9376

Clean + DP Protection Accuracy: 0.9389

Poisoned Accuracy: 0.7812

Poisoned + DP Protection Accuracy: 0.8277

Drop (Clean - Poisoned): 0.1564

Drop (Clean - Init): -0.0069

Drop (Clean DP - Init): -0.0056

Drop (Poisoned - Init): -0.1633

Drop (Poisoned DP - Init): -0.1168

DP Protection Method: trimmed_mean

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9398

Clean Recall: 0.9376

Clean F1 Score: 0.9375

Clean DP Precision: 0.9407

Clean DP Recall: 0.9389

Clean DP F1 Score: 0.9387

Poisoned Precision: 0.9017

Poisoned Recall: 0.7719

Poisoned F1 Score: 0.8066

DP Protection Precision: 0.9018

DP Protection Recall: 0.8203

DP Protection F1 Score: 0.8439

Summary

FL Simulation Complete
Task: 2dee830d-0df5-4abf-b4c5-2f50b28f94c7
GPU: GPU 0
Init Accuracy: 0.9445
Clean Accuracy: 0.9376
Clean DP Accuracy: 0.9389
Poisoned Accuracy: 0.7812
Data Poison Protection Accuracy: 0.8277
Drop (Clean - Poisoned): 0.1564
Drop (Clean - Init): -0.0069
Drop (Clean DP - Init): -0.0056
Drop (Poisoned - Init): -0.1633
Drop (Poisoned_DP - Init): -0.1168
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9398
Clean Recall: 0.9376
Clean F1 Score: 0.9375
Clean DP Precision: 0.9407
Clean DP Recall: 0.9389
Clean DP F1 Score: 0.9387
Poisoned Precision: 0.9017
Poisoned Recall: 0.7719
Poisoned F1 Score: 0.8066
DP Protection Precision: 0.9018
DP Protection Recall: 0.8203
DP Protection F1 Score: 0.8439