

FL Simulation Results

File: test1.1_BadNets_Krum

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: backdoor_badnets

Attack Intensity: 15.0% (0.15)

Poisoned Data Percentage: 30.0% (0.30)

Attack Summary: Using backdoor_badnets 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: 0.9492

Clean + DP Protection Accuracy: 0.9254

Poisoned Accuracy: 0.9545

Poisoned + DP Protection Accuracy: 0.9337

Drop (Clean - Poisoned): -0.0053

Drop (Clean - Init): 0.0047

Drop (Clean DP - Init): -0.0191

Drop (Poisoned - Init): 0.0100

Drop (Poisoned DP - Init): -0.0108

DP Protection Method: krum

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9491
Clean Recall: 0.9492
Clean F1 Score: 0.9491

Clean DP Precision: 0.9262
Clean DP Recall: 0.9254
Clean DP F1 Score: 0.9254

Poisoned Precision: 0.9544
Poisoned Recall: 0.9545
Poisoned F1 Score: 0.9543

DP Protection Precision: 0.9343
DP Protection Recall: 0.9337
DP Protection F1 Score: 0.9338

Summary

FL Simulation Complete
Task: 9d58e7f7-4f0f-4017-b46d-6167975cceb3
GPU: GPU 0
Init Accuracy: 0.9445
Clean Accuracy: 0.9492
Clean DP Accuracy: 0.9254
Poisoned Accuracy: 0.9545
Data Poison Protection Accuracy: 0.9337
Drop (Clean - Poisoned): -0.0053
Drop (Clean - Init): 0.0047
Drop (Clean DP - Init): -0.0191
Drop (Poisoned - Init): 0.0100
Drop (Poisoned_DP - Init): -0.0108
Data Poison Protection Method: krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9491
Clean Recall: 0.9492
Clean F1 Score: 0.9491
Clean DP Precision: 0.9262
Clean DP Recall: 0.9254
Clean DP F1 Score: 0.9254
Poisoned Precision: 0.9544
Poisoned Recall: 0.9545
Poisoned F1 Score: 0.9543
DP Protection Precision: 0.9343
DP Protection Recall: 0.9337
DP Protection F1 Score: 0.9338