

FL Simulation Results

File: test1.1_SmallTest

Federated Learning Configuration

Total Clients (N): 3
Malicious Clients (M): 1
Neural Network: Test1.1_
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: 0.9445
Clean Accuracy: 0.9439
Clean + DP Protection Accuracy: 0.0000
Poisoned Accuracy: 0.8192
Poisoned + DP Protection Accuracy: 0.0000
Drop (Clean - Poisoned): 0.1247
Drop (Clean - Init): -0.0006
Drop (Clean DP - Init): -0.9445
Drop (Poisoned - Init): -0.1253
Drop (Poisoned DP - Init): -0.9445
DP Protection Method: trimmed_mean
GPU Used: GPU 2

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9441
Clean Recall: 0.9439
Clean F1 Score: 0.9437

Clean DP Precision: 0.0000
Clean DP Recall: 0.0000
Clean DP F1 Score: 0.0000

Poisoned Precision: 0.7803
Poisoned Recall: 0.8192
Poisoned F1 Score: 0.7754

DP Protection Precision: 0.0000
DP Protection Recall: 0.0000
DP Protection F1 Score: 0.0000

Summary

FL Simulation Complete
Task: 2a3da21d-078c-4c1d-af81-b4c7102f505a
GPU: GPU 2
Init Accuracy: 0.9445
Clean Accuracy: 0.9439
Clean DP Accuracy: 0.0000
Poisoned Accuracy: 0.8192
Data Poison Protection Accuracy: 0.0000
Drop (Clean - Poisoned): 0.1247
Drop (Clean - Init): -0.0006
Drop (Clean DP - Init): -0.9445
Drop (Poisoned - Init): -0.1253
Drop (Poisoned_DP - Init): -0.9445
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9441
Clean Recall: 0.9439
Clean F1 Score: 0.9437
Clean DP Precision: 0.0000
Clean DP Recall: 0.0000
Clean DP F1 Score: 0.0000
Poisoned Precision: 0.7803
Poisoned Recall: 0.8192
Poisoned F1 Score: 0.7754
DP Protection Precision: 0.0000
DP Protection Recall: 0.0000
DP Protection F1 Score: 0.0000