

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: 0.9313

Poisoned Accuracy: 0.7430

Poisoned + DP Protection Accuracy: 0.4512

Drop (Clean - Poisoned): 0.1883

Drop (Clean - Init): -0.0132

Drop (Poisoned - Init): -0.2015

Drop (Poisoned DP - Init): -0.4933

DP Protection Method: krum

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9344

Clean Recall: 0.9313

Clean F1 Score: 0.9315

Poisoned Precision: 0.7653

Poisoned Recall: 0.7662

Poisoned F1 Score: 0.7609

DP Protection Precision: 0.7117

DP Protection Recall: 0.4451

DP Protection F1 Score: 0.4452

Summary

FL Simulation Complete

Task: 1f4c9f07-b62e-45a2-ab7c-86333339fdb5

GPU: GPU 0

Init Accuracy: 0.9445

Clean Accuracy: 0.9313

Poisoned Accuracy: 0.7430

Data Poison Protection Accuracy: 0.4512

Drop (Clean - Poisoned): 0.1883

Drop (Clean - Init): -0.0132

Drop (Poisoned - Init): -0.2015

Drop (Poisoned_DP - Init): -0.4933

Data Poison Protection Method: krum

--- Confusion Matrix Metrics (Weighted Avg) ---

Clean Precision: 0.9344

Clean Recall: 0.9313

Clean F1 Score: 0.9315

Poisoned Precision: 0.7653

Poisoned Recall: 0.7662

Poisoned F1 Score: 0.7609

DP Protection Precision: 0.7117

DP Protection Recall: 0.4451

DP Protection F1 Score: 0.4452