FL Simulation Results

File: test1.1_tf_Trimmed+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: 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: 0.0000

Clean Accuracy: 0.8653

Poisoned Accuracy: 0.6934

Poisoned + DP Protection Accuracy: 0.6649

Drop (Clean - Poisoned): 0.1719

Drop (Clean - Init): 0.8653

Drop (Poisoned - Init): 0.6934

Drop (Poisoned DP - Init): 0.6649

DP Protection Method: trimmed_mean_krum

GPU Used: GPU 1

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.8653

Clean Recall: 0.8653

Clean F1 Score: 0.8648

Poisoned Precision: 0.6906

Poisoned Recall: 0.7160

Poisoned F1 Score: 0.7003

DP Protection Precision: 0.6939

DP Protection Recall: 0.6822

DP Protection F1 Score: 0.6832

Summary

FL Simulation Complete
Task: 49d218e4-af09-4628-a44a-f84e79254504
GPU: GPU 1
Init Accuracy: 0.0000
Clean Accuracy: 0.8653
Poisoned Accuracy: 0.6934
Data Poison Protection Accuracy: 0.6649
Drop (Clean - Poisoned): 0.1719
Drop (Clean - Init): 0.8653
Drop (Poisoned - Init): 0.6934
Drop (Poisoned_DP - Init): 0.6649
Data Poison Protection Method: trimmed_mean_krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.8653
Clean Recall: 0.8653
Clean F1 Score: 0.8648
Poisoned Precision: 0.6906
Poisoned Recall: 0.7160
Poisoned F1 Score: 0.7003
DP Protection Precision: 0.6939
DP Protection Recall: 0.6822
DP Protection F1 Score: 0.6832