FL Simulation Results

File: test1.1_New_Network

Federated Learning Configuration

Total Clients (N): 2

Malicious Clients (M): 1

Neural Network: MyNN

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: 0.3711

Clean Accuracy: 0.9104

Poisoned Accuracy: 0.1703

Poisoned + DP Protection Accuracy: 0.1554

Drop (Clean - Poisoned): 0.7401

Drop (Clean - Init): 0.5393

Drop (Poisoned - Init): -0.2008

Drop (Poisoned DP - Init): -0.2157

DP Protection Method: fedavg

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9258
Clean Recall: 0.9144
Clean F1 Score: 0.9104

Poisoned Precision: 0.2008
Poisoned Recall: 0.1269
Poisoned F1 Score: 0.0727

DP Protection Precision: 0.1049
DP Protection Recall: 0.1123
DP Protection F1 Score: 0.0483

Summary

FL Simulation Complete
Task: 0503a022-04ee-4fa6-a671-d8b03878dcd4
GPU: GPU 0
Init Accuracy: 0.3711
Clean Accuracy: 0.9104
Poisoned Accuracy: 0.1703
Data Poison Protection Accuracy: 0.1554
Drop (Clean - Poisoned): 0.7401
Drop (Clean - Init): 0.5393
Drop (Poisoned - Init): -0.2008
Drop (Poisoned_DP - Init): -0.2157
Data Poison Protection Method: fedavg
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9258
Clean Recall: 0.9144
Clean F1 Score: 0.9104
Poisoned Precision: 0.2008
Poisoned Recall: 0.1269
Poisoned F1 Score: 0.0727
DP Protection Precision: 0.1049
DP Protection Recall: 0.1123
DP Protection F1 Score: 0.0483