FL Simulation Results

File: Label_Flip_10

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: 0.9495

Clean + DP Protection Accuracy: 0.9291

Poisoned Accuracy: 0.9256

Poisoned + DP Protection Accuracy: 0.8485

Drop (Clean - Poisoned): 0.0239

Drop (Clean - Init): 0.0050

Drop (Clean DP - Init): -0.0154

Drop (Poisoned - Init): -0.0189

Drop (Poisoned DP - Init): -0.0960

DP Protection Method: krum

GPU Used: GPU 1

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9495

Clean Recall: 0.9495

Clean F1 Score: 0.9494

Clean DP Precision: 0.9293

Clean DP Recall: 0.9291

Clean DP F1 Score: 0.9290

Poisoned Precision: 0.9275

Poisoned Recall: 0.9256

Poisoned F1 Score: 0.9259

DP Protection Precision: 0.8778

DP Protection Recall: 0.8485

DP Protection F1 Score: 0.8549

Summary

```
FL Simulation Complete
Task: e16fa0d3-4328-4ffc-8428-9f912914318e
GPU: GPU 1
Init Accuracy: 0.9445
Clean Accuracy: 0.9495
Clean DP Accuracy: 0.9291
Poisoned Accuracy: 0.9256
Data Poison Protection Accuracy: 0.8485
Drop (Clean - Poisoned): 0.0239
Drop (Clean - Init): 0.0050
Drop (Clean DP - Init): -0.0154
Drop (Poisoned - Init): -0.0189
Drop (Poisoned_DP - Init): -0.0960
Data Poison Protection Method: krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9495
Clean Recall: 0.9495
Clean F1 Score: 0.9494
Clean DP Precision: 0.9293
Clean DP Recall: 0.9291
Clean DP F1 Score: 0.9290
Poisoned Precision: 0.9275
Poisoned Recall: 0.9256
Poisoned F1 Score: 0.9259
DP Protection Precision: 0.8778
DP Protection Recall: 0.8485
DP Protection F1 Score: 0.8549
```