FL Simulation Results

File: test_demo4

Federated Learning Configuration

Total Clients (N): 2

Malicious Clients (M): 1

Neural Network: SimpleNN

Training Rounds: 2

Poisoned Rounds (R): 1

Distribution Strategy: alternate_data

Data Poisoning Attack Parameters

Poisoning Operation: backdoor_badnets

Attack Intensity: 15.0% (0.15)

Poisoned Data Percentage: 30.0% (0.30)

Attack Summary: Using backdoor_badnets 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: 0.9382

Clean + DP Protection Accuracy: 0.9249

Poisoned Accuracy: 0.9451

Poisoned + DP Protection Accuracy: 0.9342

Drop (Clean - Poisoned): -0.0069

Drop (Clean - Init): -0.0063

Drop (Clean DP - Init): -0.0196

Drop (Poisoned - Init): 0.0006

Drop (Poisoned DP - Init): -0.0103

DP Protection Method: krum

GPU Used: GPU 0

Confusion Matrix Metrics (Weighted Avg):

Clean Precision: 0.9383
Clean Recall: 0.9382
Clean F1 Score: 0.9380

Clean DP Precision: 0.9252
Clean DP Recall: 0.9249
Clean DP F1 Score: 0.9247

Poisoned Precision: 0.9454
Poisoned Recall: 0.9451
Poisoned F1 Score: 0.9451

DP Protection Precision: 0.9353
DP Protection Recall: 0.9342
DP Protection F1 Score: 0.9338

Summary

```
FL Simulation Complete
Task: 7800b125-dd92-4166-8512-f92bbde56101
GPU: GPU 0
Init Accuracy: 0.9445
Clean Accuracy: 0.9382
Clean DP Accuracy: 0.9249
Poisoned Accuracy: 0.9451
Data Poison Protection Accuracy: 0.9342
Drop (Clean - Poisoned): -0.0069
Drop (Clean - Init): -0.0063
Drop (Clean DP - Init): -0.0196
Drop (Poisoned - Init): 0.0006
Drop (Poisoned_DP - Init): -0.0103
Data Poison Protection Method: krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.9383
Clean Recall: 0.9382
Clean F1 Score: 0.9380
Clean DP Precision: 0.9252
Clean DP Recall: 0.9249
Clean DP F1 Score: 0.9247
Poisoned Precision: 0.9454
Poisoned Recall: 0.9451
Poisoned F1 Score: 0.9451
DP Protection Precision: 0.9353
DP Protection Recall: 0.9342
DP Protection F1 Score: 0.9338
```