# FL Simulation Results

File: test1.1_Trojan

## 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: backdoor_trojan

Attack Intensity: 15.0% (0.15)

Poisoned Data Percentage: 30.0% (0.30)

*Attack Summary: Using backdoor_trojan with 15.0% (0.15) intensity on 30.0% (0.30) of data for 5 rounds with 1 malicious clients.*

## Simulation Results

Init Accuracy: 0.7334

Clean Accuracy: 0.8619

Poisoned Accuracy: 0.8303

Poisoned + DP Protection Accuracy: 0.8296

Drop (Clean - Poisoned): 0.0316

Drop (Clean - Init): 0.1285

Drop (Poisoned - Init): 0.0969

Drop (Poisoned DP - Init): 0.0962

DP Protection Method: trimmed_mean

GPU Used: GPU 1

**Confusion Matrix Metrics (Weighted Avg):**

Clean Precision: 0.8623

Clean Recall: 0.8619

Clean F1 Score: 0.8613

Poisoned Precision: 0.8307

Poisoned Recall: 0.8334

Poisoned F1 Score: 0.8306

DP Protection Precision: 0.8299

DP Protection Recall: 0.8307

DP Protection F1 Score: 0.8282

## Summary

FL Simulation Complete
Task: 30a510cc-6dca-490a-8edc-b80bee63ffbc
GPU: GPU 1
Init Accuracy: 0.7334
Clean Accuracy: 0.8619
Poisoned Accuracy: 0.8303
Data Poison Protection Accuracy: 0.8296
Drop (Clean - Poisoned): 0.0316
Drop (Clean - Init): 0.1285
Drop (Poisoned - Init): 0.0969
Drop (Poisoned_DP - Init): 0.0962
Data Poison Protection Method: trimmed_mean
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.8623
Clean Recall: 0.8619
Clean F1 Score: 0.8613
Poisoned Precision: 0.8307
Poisoned Recall: 0.8334
Poisoned F1 Score: 0.8306
DP Protection Precision: 0.8299
DP Protection Recall: 0.8307
DP Protection F1 Score: 0.8282