# FL Simulation Results

File: test1_tf

## Federated Learning Configuration

Total Clients (N): 5

Malicious Clients (M): 3

Neural Network: MyNN

Training Rounds: 5

Poisoned Rounds (R): 3

Distribution Strategy: first

## Data Poisoning Attack Parameters

Poisoning Operation:  Label Flip

Attack Intensity: 10.0% (0.10)

Poisoned Data Percentage: 20.0% (0.20)

*Attack Summary: Using label_flip with 10.0% (0.10) intensity on 20.0% (0.20) of data for 3 rounds with 3 malicious clients.*

## Simulation Results

Init Accuracy: 0.7334

Clean Accuracy: 0.8565

Poisoned Accuracy: 0.7038

Poisoned + DP Protection Accuracy: 0.6882

Drop (Clean - Poisoned): 0.1527

Drop (Clean - Init): 0.1231

Drop (Poisoned - Init): -0.0296

Drop (Poisoned DP - Init): -0.0452

DP Protection Method: krum

GPU Used: GPU 0

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

Clean Precision: 0.8596

Clean Recall: 0.8565

Clean F1 Score: 0.8557

Poisoned Precision: 0.7028

Poisoned Recall: 0.7169

Poisoned F1 Score: 0.7058

DP Protection Precision: 0.6839

DP Protection Recall: 0.7012

DP Protection F1 Score: 0.6875

## Summary

FL Simulation Complete
Task: a9df2cba-864f-4a04-a2f9-1452c5ea3b83
GPU: GPU 0
Init Accuracy: 0.7334
Clean Accuracy: 0.8565
Poisoned Accuracy: 0.7038
Data Poison Protection Accuracy: 0.6882
Drop (Clean - Poisoned): 0.1527
Drop (Clean - Init): 0.1231
Drop (Poisoned - Init): -0.0296
Drop (Poisoned_DP - Init): -0.0452
Data Poison Protection Method: krum
--- Confusion Matrix Metrics (Weighted Avg) ---
Clean Precision: 0.8596
Clean Recall: 0.8565
Clean F1 Score: 0.8557
Poisoned Precision: 0.7028
Poisoned Recall: 0.7169
Poisoned F1 Score: 0.7058
DP Protection Precision: 0.6839
DP Protection Recall: 0.7012
DP Protection F1 Score: 0.6875