Cluster : Fintech Security (incl. Blockchain)

Problem Statement title : Mule Accounts & Collusive Fraud in UPI

Description:

Develop a real-time fraud detection system to identify mule accounts and collusive fraud networks in UPI and instant payment platforms. The solution should leverage advanced techniques like graph-based transaction analytics, device fingerprinting, identity attribute correlation, and real-time risk scoring APIs, that can detect fraudulent clusters early, minimize false positives, and integrate seamlessly with India's high-volume payment infrastructure.

Exact Deliverables :

- Prototype for detecting mule accounts using transaction graph features and device fingerprints.

- Model for spotting collusive fraud patterns (money-mule rings) across UPI flows.

- Precision/recall evaluation report on fraud detection performance.

- Dashboard or visualization layer to track suspicious clusters of accounts.

Milestones, Evolution Parameters:

- Phase 1: Build baseline fraud detection using transaction rules.

- Phase 2: Implement graph-based anomaly detection and device fingerprinting.

- Phase 3: Deploy real-time API for risk scoring in simulated UPI flows.

- KPIs: Detection accuracy, false positive rate, average detection latency, scalability to millions of transactions.

Additional Information:

- Students should emphasize scalability and integration with real-time payment rails.

- Techniques from fraud graph learning and behavioral analysis should be explored.

- Visualization of fraud networks will enhance usability for investigators.