FinGuard: Real-Time Mule Account Detection System for UPI Payments

Team Submission for Cyber Security Innovation Challenge 1.0

Team Mandelbrot

Problem Statement: Mule Accounts & Collusive Fraud in UPI

Date: December 28, 2025

1 Introduction

The UPI payment ecosystem continues to grow rapidly, making fraud detection increasingly challenging. Most current systems rely on static rules that evaluate transactions in isolation, which allows mule account operations to remain hidden across multiple transfers. These operations disrupt fund traceability and reduce visibility into the payment network.

Graph based analysis helps reveal relationships between accounts that are missed by rule based systems. When combined with temporal behavior tracking and device level signals, it becomes possible to identify coordinated fraud patterns rather than isolated suspicious transactions. Motivated by this, we propose a hybrid detection system that brings these signals together to improve mule account detection while keeping false positives low.

2 System and Adversary Model

2.1 Traditional Payment System Model

A UPI payment network is a combination of user accounts and banking infrastructure that work together to support digital transactions. User accounts initiate and receive payments through UPI applications, while the banking infrastructure is responsible for processing and validating these transactions. Fraud detection systems monitor the network to ensure secure operation and mainly rely on rule based engines for real-time checks.. These systems exchange monitoring information with the payment infrastructure using protocols defined under UPI specifications.

2.2 Attack Model and Problem Statement

Since user accounts and banking infrastructure operate over shared networks, this connectivity can be exploited by fraudsters as an entry point. Adversaries create mule account networks that move funds through multiple intermediary accounts, which disrupt fund traceability.When viewed individually each transaction appears legitimate , causing the static rule based systems to miss the overall fraud pattern. As a result, coordinated mule account operations remain undetected, leading to delayed response, financial losses, and reduced situational awareness.

3 System Architecture

3.1 Overall Architecture

Fig. 1 shows the proposed fraud detection architecture for a UPI payment network. Incoming UPI transactions would be first collected through a real time ingestion layer using **Kafka**. A feature engineering stage would then enriches each transaction with behavioral, graph, and device related information.

The enriched data would be processed by a multi model scoring engine that combines temporal analysis, transaction graph patterns, and device correlation. The resulting risk scores would be aggregated using weighted thresholds, and suspicious activity is presented to investigators through a dashboard for review. Recent data is cached in **Redis**, to support low latency processing, while transaction graphs and historical records are stored in **Neo4j** and **PostgreSQL**.

The architecture separates real time processing from batch processing. Recent transaction patterns and device mappings (Hot data) are cached in **Redis** for fast access. Transaction Graph structures are planned to be maintained in **Neo4j** to efficiently support network queries . **PostgreSQL** is used as the persistent storage for audit logs and historical data.

3.2 Data Flow

Transactions would move through ingestion, enrichment, and scoring stages in sequence. Temporal, graph, and device based checks would run in parallel, and their outputs are combined into a single risk score. High risk cases would be surfaced immediately for investigation, while lower risk cases are handled offline. Aggregation thresho lds are adjusted based on transaction context, such as account age and recent activity.

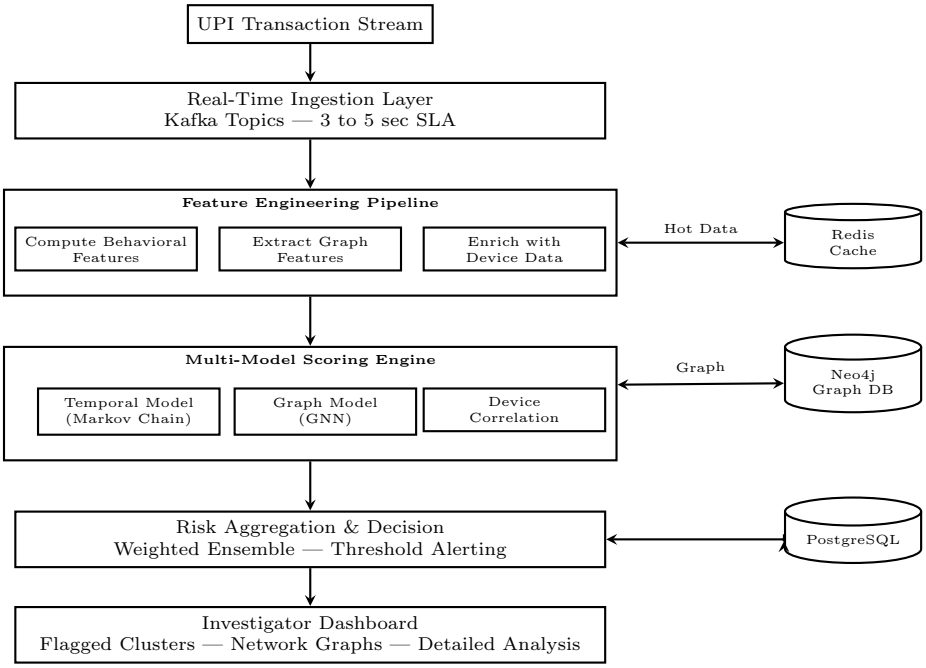

Figure 1: System Architecture for Real-Time Mule Account Detection

4 Detection Methodology

4.1 Temporal Behavior Tracking

The temporal component analyzes how account behavior changes over time and highlights patterns associated with mule activity. Each account is tracked using basic transaction patterns such as inflow, outflow, transaction frequency, amount ranges, and time of activity. Sudden deviations from past behavior increase the risk score. This module is designed using a **Markov Chain** based model that captures short term behavioral transitions, helping detect dormant accounts that suddenly become active or accounts that forward funds immediately without normal usage. This behavior is especially noticeable in accounts with little prior activity, where even small deviations become meaningful.

4.2 Graph Neural Network Analysis

Coordinated fraud is examined by modeling transactions as graphs where accounts act as nodes and UPI transfers form edges. Mule account networks often show recognizable patterns such as star shaped aggregation, sequential laundering chains, or circular fund movement. These patterns are analyzed using graph features and a Graph Neural Network to distinguish organized mule operations from normal transaction behavior. Transaction graphs are planned to be stored and queried using Neo4j for efficient network level analysis.In practice, three primary patterns are commonly associated with mule operations:

1. **Star Pattern**: A central account receives funds from multiple sources and then forwards to a single destination,which often indicates aggregation of stolen funds.
2. **Chain Pattern**: Funds move sequentially through a series of intermediary accounts,forming a laundering chain that intended to hide the original source.
3. **Circular Pattern**: Funds loop back to the origin after multiple hops, indicating test transactions or layering schemes.

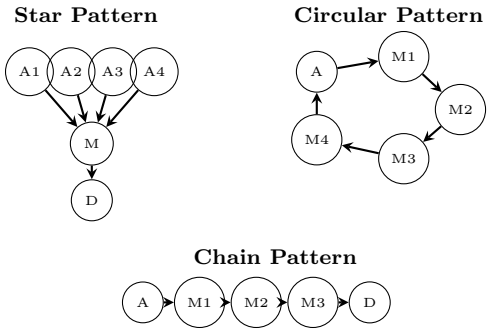

Figure 2: Fraud Patterns in Mule Account Networks

Fig. 2 shows these three fraud patterns that are commonly observed in mule account networks.

4.3 Device Fingerprinting

Device fingerprinting helps link multiple accounts controlled from the same device. Signals such as device identifiers, login patterns, and access context are used to associate accounts with shared devices. When suspicious behavior is

detected on one account, risk scores can be propagated across linked accounts. Fast lookup of device to account mappings is supported using Redis.

4.4 Real-Time Scoring

UPI latency requirements require a lightweight real time scoring approach, combined with deeper asynchronous analysis. Incoming transactions would be scored using cached behavioral, graph, and device level signals, allowing quick decisions without delaying payments. Streaming would be handled through Kafka, while scoring services are exposed through **FastAPI**. Historical past records and audit data would be maintained in PostgreSQL for long term analysis and review.

5 Expected Outcomes and Benchmarking

This system is designed to detects fraud more efficiently than traditional rule based engines and is more dependable than isolated ML models.The approach is expected to maintain precision under real world UPI traffic which results in higher detection rates while keeping precision stable. This allows legitimate users to experience minimal disturbance. The platform is designed to work within the time limits of current UPI transactions. It is intended to enable risk scoring in real-time without any noticeable delays. Early detection of mules could allow banks to react faster to fraud operations resulting in lower financial losses.

Currently fraud detection techniques are mainly based on two approaches: static rule based systems and classic machine learning models. Rule based systems provide instant decisions that are easy to understand, but they are inflexible and unable to adapt to new fraud patterns. Machine learning models have better pattern recognition but lack transparency and still face difficulties with network level fraud. The proposed system addresses this through integration of temporal behavior modeling, transaction network analysis, and device level correlation within a single framework.

Table 1: Comparison with Existing Approaches

Feature	**Rules**	**ML**	**Hybrid**
Temporal Patterns	Static	Limited	Full
Network Analysis	None	None	GNN
Device Correlation	None	None	Yes
Real-time Scoring	Fast	Moderate	Fast
Explainability	Clear	Black box	Clear
Adaptation	Manual	Periodic	Continuous

Table 1 presents comparison across key capabilities. The proposed solution provides coverage of temporal patterns, network analysis, and device correlation—capabilities that are absent or limited in existing approaches.

6 Differentiation and Value Proposition

One of the main features that sets this system apart is its multi signal detection strategy. Behavioral patterns help surface individual mule activity, but coordinated fraud becomes visible only when transaction graph analysis and device level signals are considered together. This method detects a wider range of fraud scenarios than single model systems. Explainability is an integral part where every alert contains reasons that investigators, customers, and regulators can understand. This transparency is important for adoption in regulated financial environments.

The system is designed for the scale and dynamics of India's UPI ecosystem. Architectural choices such as horizontal scaling, adaptive thresholds based on account maturity, and separation of batch and real-time processing contribute to resilience during high transaction volumes. The focus on deployment practicality and long term adaptability differentiates this from academic solutions.

7 Product Roadmap and End-Use Cases

The roadmap begins with minimum viable monitoring and gradually introduces more advanced detection capabilities. The initial stage, spanning the first few weeks, focuses on setting up transaction monitoring and basic alerting. In the following stage, attention shifts to adding temporal behavior analysis to capture changes in account activity over time. The next phase introduces transaction graph analysis, with an emphasis on identifying coordinated fraud patterns across multiple accounts. In the final stage, device fingerprinting is integrated with the real-time pipeline to strengthen cross account correlation and detection.

End use cases include individual and organized fraud scenarios. Student mule accounts represent cases where students are unwittingly used in job scams where the system detects dormant accounts suddenly receiving and forwarding large amounts. Organized fraud rings involve operations running multiple coordinated accounts where graph analysis identifies complete network structure. Compromised legitimate customers represent cases where accounts are taken over and device fingerprinting detects login from new devices with unusual patterns. Layering operations involve criminals using circular money flows where the GNN model recognizes patterns that traditional systems miss.

8 Conclusion

We proposed a hybrid detection system for mule account identification in UPI combining temporal tracking, graph analysis, and device correlation. The hybrid system allows fraud detection even when individual methods may generate

false alarms. The proposed approach highlights the potential advantages of using multi signal validation with much lower false positive percentages compared to single method approaches.

The system is designed as decision support rather than fully automated blocking, ensuring conservative intervention during early deployment. This approach allows human investigators to validate recommendations and provide feedback that improves detection accuracy while minimizing disruption to legitimate users.

References

[1] G. Jambhrunkar et al., "MuleTrack: A Lightweight Temporal Learning Framework for Money Mule Detection," in *Proceedings of IWANN*, 2025.

[2] D. Cheng et al., "Graph Neural Networks for Financial Fraud Detection: A Review," *arXiv preprint arXiv:2411.05815*, 2024.

[3] M. Caglayan and S. Bahtiyar, "Money Laundering Detection with Node2Vec," *Gazi University Journal of Science*, vol. 35, no. 3, pp. 854–873, 2022, doi: 10.35378/gujs.854725.

[4] Z. Huang, "Enhancing Anti-Money Laundering by Money Mules Detection on Transaction Graphs," in *Proc. 2025 Int. Conf. on Generative Artificial Intelligence for Business (GAIB)*, ACM, Hong Kong, China, Aug. 2025, doi: 10.1145/3766918.3766933.

[5] Neo4j Inc., "Accelerate Fraud Detection with Graph Databases," Whitepaper, 2023. [Online]. Available: https://neo4j.com

[6] Confluent Inc., "Real-Time Fraud Detection in Banking," Whitepaper, 2023. [Online]. Available: https://www.confluent.io :contentReference[oaicite:0]index=0

[7] National Payments Corporation of India, "Annual Report 2024 - UPI Transaction Statistics," NPCI, 2024.

[8] National Payments Corporation of India, "Unified Payment Interface: API and Technology Specifications," Version 1.2.3, 2023. [Online]. Available: https://www.npci.org.in