बैंक ऑफ़ बड़ौदा
Bank of Baroda

वित्तीय सेवाएं विभाग
DEPARTMENT OF
FINANCIAL SERVICES

PROJECT OVERVIEW

1. Title & Team details
2. Problem statement
3. Outline of Unique & innovative solution
4. Business model and commercialization potential
5. Proposed process flow / Architecture of implementation
6. Algorithm Details
7. One-page summary of the project

1. Title & Team Details

Title: CAI-Powered User & Entity Behaviour Analytics (UEBA) for Fraud Detection

Team Name: INNOVATOR

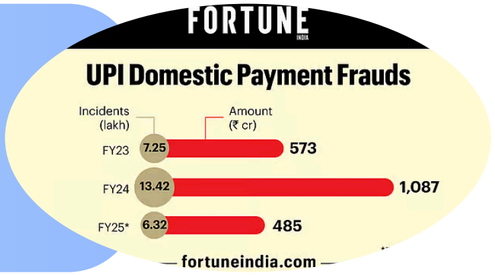
Name: Kritnandan
(Team Leader)
kritnandan22@iitk.ac.in
7800060023

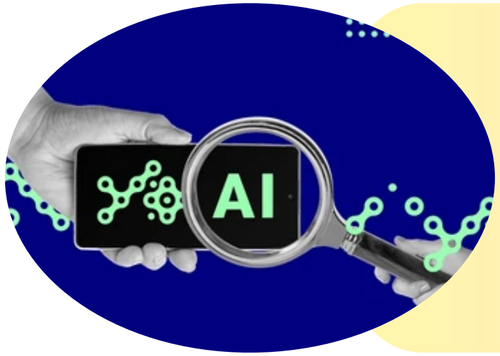
Name: Abhijit Dalai
abhijitd22@iitk.ac.in
7008793484

Name: Khushi Tiwari
khushiti22@iitk.ac.in
7008032518

2. Problem Statement

With digital banking spanning internet, mobile apps, UPI, ATMs, and APIs, fraud risks are at an all-time high. In India alone, digital payment fraud reached **₹14.57 billion** in **FY 2023-24**, with UPI scams causing losses of **₹485 crore** across **6.3 lakh** cases.





Evolving fraud schemes (**Account Takeover**, **synthetic/new-account** fraud, **mule networks** via recruited mules) evade static rules. Traditional rule-based systems often miss such fraud patterns and generate up to **95%** false positives, degrading customer trust and experience. This highlights the urgent need for **AI-powered** behavioral analytics to detect fraud more accurately, with contextual and network awareness.

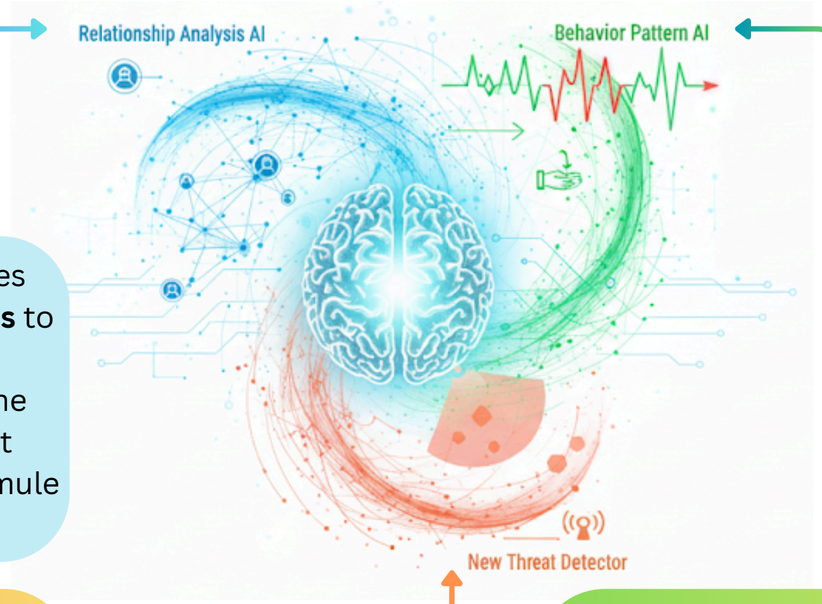
Sources:

- https://www.businesstoday.in/technology/news/story/digital-payment-frauds-surge-in-india-as-upi-transactions-skyrocket-rbi-report-431695-2024-06-01?utm
- https://www.fortuneindia.com/macro/upi-frauds-63-lakh-cases-worth-485-cr-reported-in-fy25-so-far/119275
- https://www.retailbankerinternational.com/comment/hidden-cost-of-aml-how-false-positives-hurt-banks-fintechs-customers/?cf-view

3. Outline of Unique & Innovative Solution

A 3-in-1 Smart Detection Engine

Three layers of specialized AI for comprehensive threat coverage



Links accounts and devices across **14,000+ transactions** to reveal hidden network relationships, providing the context needed to detect **coordinated fraud** such as mule rings

Provides an **unsupervised safety net**, capable of identifying novel and **emerging fraud typologies** that supervised models have not been trained to recognize

Learns each customer's unique **digital rhythm** to flag account takeovers by tracking recency, 1h/24h/7d transaction velocity, and deviations from usual spend

Self-Learning Decision Engine

The engine moves beyond static rules and learns from the outcome of every transaction, adapting its response to be more effective over time

Instead of a simple "block" or "approve" rule, our model learns the **optimal action** for each specific context, choosing between:

Approve	Challenge	Block
Low-risk	Medium-risk	High-risk

Projected Impact

- **30–40%** reduction in false positives
- **50%** faster fraud detection vs. legacy rules
- **Improved CX** – fewer unnecessary blocks/challenges
- Adaptive performance – **gets smarter** with every transaction

बैंक ऑफ़ बड़ौदा
Bank of Baroda

वित्तीय सेवाएं विभाग
DEPARTMENT OF
FINANCIAL SERVICES

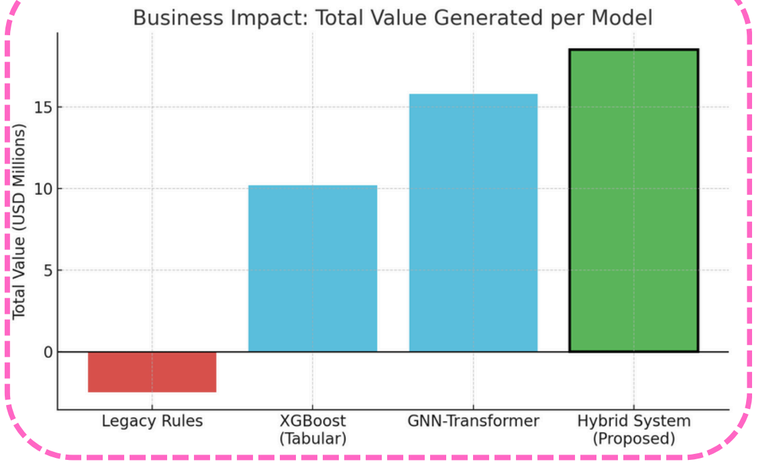
4. Business model and commercialization potential

Market
Banks, **NBFCs**, **fintechs**, and **payment service providers (PSPs)** handling millions of daily transactions

Pain Points
Rising **fraud losses**, **false positives** hurting CX, and **outdated rule engines** failing to adapt

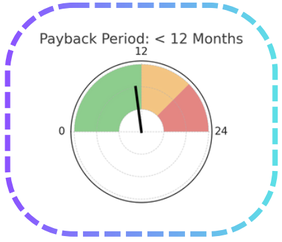
Solution
Hybrid AI engine + Reinforcement Learning

Revenue
SaaS + Enterprise Licenses + Services



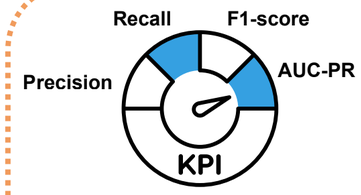
Performance Benchamarks against Baseline Models

Model	Precision	Recall	F1-score	AUC-PR	Total Value
Legacy Rule-Based System	0.15	0.45	0.23	0.3	-$2.5M
XGBoost (Tabular Features)	0.65	0.6	0.62	0.75	+$10.2M
GNN-Transformer (Supervised)	0.82	0.75	0.78	0.88	+$15.8M
Full Hybrid System with Contextual Bandits (Proposed)	0.85	0.8	0.82	0.91	+$18.5M



Accuracy alone is misleading, **choosing the right metrics**:

- **Precision-Recall & AUC-PR**: Balance fraud detection vs. false positives
- **Recall @ Low FPR (<1%)**: Maximize fraud catch rate without hurting CX
- **F1-Score**: Optimal trade-off between precision and recall

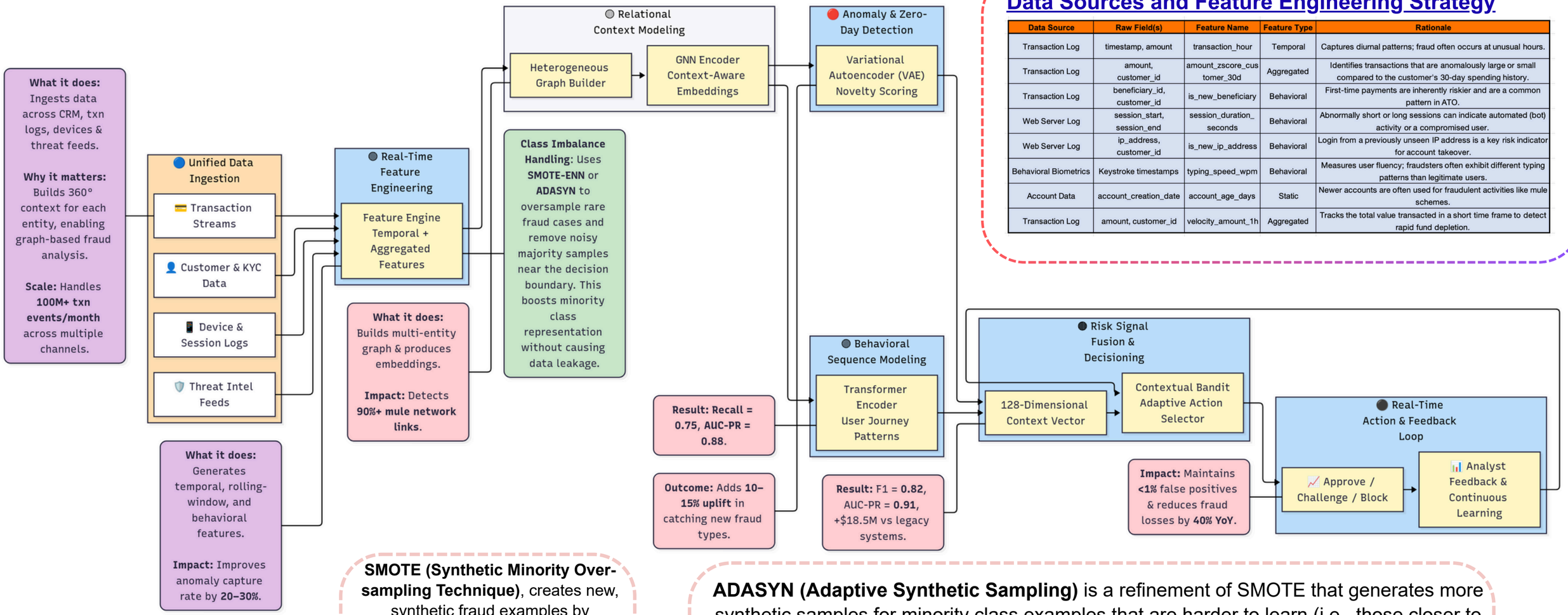


Key Performance Indicators

Scalability and Real-time Inference

- **Ultra-Low Latency:** Optimized inference (<100 ms) using NVIDIA Triton servers for concurrent, high-throughput requests.
- **Model Optimization:** Quantization & pruning to reduce compute cost without losing accuracy.
- **Fast Graph Operations:** In-memory graph caching & efficient subgraph sampling for real-time GNN inference.
- **Continuous Monitoring:** Real-time dashboards tracking Precision, Recall, F1-score, fraud loss rates & false positives.
- **Drift Detection:** Contextual Bandit rewards signal concept drift, triggering model retraining when needed.
- **Explainability (XAI):** SHAP-based feature attribution + graph visualizations to meet regulatory requirements and accelerate investigations.
- **Human-in-the-Loop:** AI handles routine cases; complex alerts routed to analysts with full context for faster resolution.
- **Closed Feedback Loop:** Analyst outcomes retrain models & update RL policy — making the system continuously smarter.

5. Proposed process flow / Architecture of implementation



Data Sources and Feature Engineering Strategy

Data Source	Raw Field(s)	Feature Name	Feature Type	Rationale
Transaction Log	timestamp, amount	transaction_hour	Temporal	Captures diurnal patterns; fraud often occurs at unusual hours.
Transaction Log	amount, customer_id	amount_zscore_customer_30d	Aggregated	Identifies transactions that are anomalously large or small compared to the customer's 30-day spending history.
Transaction Log	beneficiary_id, customer_id	is_new_beneficiary	Behavioral	First-time payments are inherently riskier and are a common pattern in ATO.
Web Server Log	session_start, session_end	session_duration_seconds	Behavioral	Abnormally short or long sessions can indicate automated (bot) activity or a compromised user.
Web Server Log	ip_address, customer_id	is_new_ip_address	Behavioral	Login from a previously unseen IP address is a key risk indicator for account takeover.
Behavioral Biometrics	Keystroke timestamps	typing_speed_wpm	Behavioral	Measures user fluency; fraudsters often exhibit different typing patterns than legitimate users.
Account Data	account_creation_date	account_age_days	Static	Newer accounts are often used for fraudulent activities like mule schemes.
Transaction Log	amount, customer_id	velocity_amount_1h	Aggregated	Tracks the total value transacted in a short time frame to detect rapid fund depletion.

SMOTE (Synthetic Minority Over-sampling Technique), creates new, synthetic fraud examples by interpolating between existing fraud instances in the feature space.

ADASYN (Adaptive Synthetic Sampling) is a refinement of SMOTE that generates more synthetic samples for minority class examples that are harder to learn (i.e., those closer to the decision boundary), adaptively focusing the model on the most difficult cases.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

वित्तीय सेवाएं विभाग
DEPARTMENT OF
FINANCIAL SERVICES

6. Algorithm Details

How **Reinforcement Learning** works here:

- **Context**: 128-D risk vector (GNN + Transformer + VAE + features).
- **Action**: Selects Approve / 2FA / Block.
- **Reward**: Positive if fraud is blocked, negative if missed or customer unnecessarily challenged.
- **Learning**: Continously learns optimal actions by balancing exploration vs. exploitation to maximize reward.

Time-window aggregations: rolling mean/median/sum/count, std/volatility (1h/24h/7d/30d)

Velocity & burst metrics, Recency/Frequency/Monetary (**RFM**), scaling & **normalization**

Node Types: User, Account, Transaction, Device, IP Address, Merchant.

Edge Types: Capture relationships like (User–owns–Account), (Account–sent–Transaction), (Transaction–initiated_from–IP).

Features: Node attributes (e.g., account_age, avg_txn_amount_30d) and edge attributes (e.g., txn amount, timestamp) enrich graph context.

Learns to choose the best action (**Approve / 2FA / Block**) for each transaction context using a **reward-based** system.

Flags zero-day or unseen frauds when **reconstruction error** is high (e.g., beyond 99th percentile of normal validation data).

Learns a **probabilistic latent space** of normal transactions by minimizing reconstruction loss + KL divergence.

Performs **k-hop message passing**, where each node aggregates information from its neighbors up to k layers deep (e.g., user → account → device → merchant).

Generates **context-aware embeddings** capturing both local and multi-hop structural context

Learns **temporal behavior patterns** (e.g., normal login → purchase → transfer flow) and flags deviations like account takeover or bot-driven fraud.

Takes GNN embeddings and processes user activity as a **time-ordered sequence** with **self-attention.**

Uses **Relational Graph Convolutional Network** (**R-GCN**) to handle multiple edge types and **Graph Attention Network** (**GAT**) attention to weigh neighbor importance.

बैंक ऑफ़ बड़ौदा
Bank of Baroda

वित्तीय सेवाएं विभाग
DEPARTMENT OF
FINANCIAL SERVICES
सत्यमेव जयते

7. One-page summary of the project

The Challenge: Digital payment fraud is rising, while legacy rule-based systems suffer from high false positives (up to 95%), poor adaptability, and weak detection of advanced threats.

Architecture & Flow:

Real-time ingestion of 100M+ events/month. → Rich feature engineering with graph embeddings & behavioral signals → Parallel AI inference producing a unified context vector. → Continuous learning loop through adaptive decisioning.

Our Solution: A 3-in-1 Smart Detection Engine powered by AI and Self-Learning Decisioning:

- **Relationship Analysis (GNNs):** Unmasks hidden fraud rings via entity networks.
- **Behavior Pattern AI (Transformers):** Detects anomalies in user transaction sequences.
- **New Threat Detection (VAE):** Identifies zero-day and unseen fraud patterns.
- **Adaptive Decisioning (Contextual Bandits):** Learns optimal actions (Approve, Challenge, Block) for continuous improvement.

Projected Impact

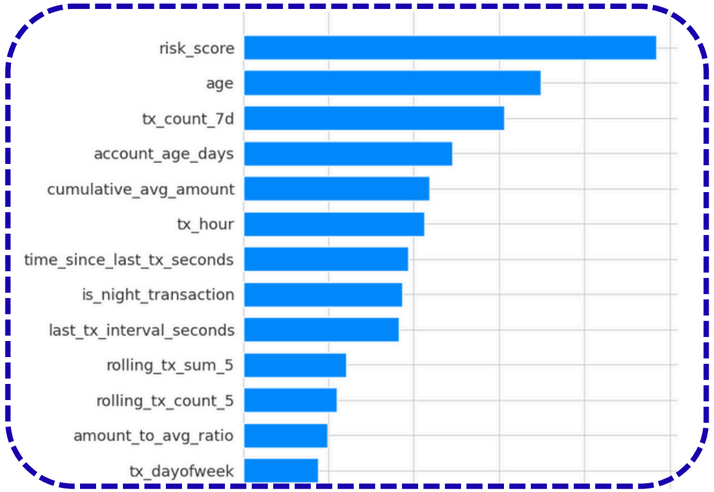
Performance Metrics:
Recall, Precision, F1-score and AUC-PR

Customer Trust:
Less friction, improved experience.

Efficiency:
30–40% fewer false positives, 50% faster detection.

Business Value:
+$18.5M ROI, SaaS-ready, <12 months payback.

Feature Importance in Fraud Detection Prediction



Conclusion: A shift from reactive fraud detection to proactive, intelligent prevention—delivering robust, adaptive, and scalable defense for Bank of Baroda's digital ecosystem.