Intent-Aware Behavioral Transaction Engine

Team Name: RJ_19 Squad
Project Title: Intent-Aware Behavioral Transaction Engine
Domain: Financial Safety
Team Members:
Nepal Singh

Vishal Suthar

1. Why did you choose this problem? (Inspiration & relevance)

- India processes over 10+ billion UPI transactions per month, making real-time safety critical
- Financial fraud losses in digital payments run into tens of thousands of crores annually
- Over 60% of reported digital fraud cases involve social engineering and user manipulation
- Most victims technically authorize the transaction themselves under pressure or fear
- No mainstream payment system evaluates human intent at the moment of payment
- This gap inspired us to focus on behavioral and psychological signals instead of static rules

2. Who is affected by this problem and how do they deal with it today?

- Primary users: UPI users across age groups, especially senior citizens and first-time digital users
- Secondary stakeholders: Banks, fintech companies, regulators, and cybercrime cells
- Banks currently rely on transaction metadata such as amount, location, and frequency
- User behavior during payment (panic, hesitation, coercion) is not deeply modeled
- Users rely on post-fraud complaint mechanisms, which rarely result in full recovery
-

3. What is the root cause of this problem? (Depth of understanding)

- Modern fraud exploits human psychology rather than breaking financial systems
- Transaction-level data cannot capture intent, stress, or coercion
- Behavioral signals exist but are not unified into a real-time intent model
- Blocking transactions aggressively leads to poor user experience and false positives
- No production system focuses on intent inference as a first-class security layer

4. How does your solution address the root cause? (Solution logic)

- Deploys an **Intent-Aware Engine** embedded directly into the payment flow **before transaction submission**, ensuring intervention happens at the decision point
- Continuously learns **user-specific behavioural baselines** from historical transaction patterns and interaction behaviour
- Extracts **multi-dimensional real-time signals**, including:
  - confirmation speed and interaction timing patterns
  - hesitation, retries, and cancel-reattempt behaviour
  - sudden transaction amount deviation from personal norms
  - abnormal transaction time and location shifts

    - rapid context switching between calls and payment apps
    - multiple incoming calls from unknown or suspicious numbers shortly before payment
    - device and network anomalies during high-risk moments
- Correlates these behavioural, contextual, and temporal signals using **machine-learning models** to infer whether the user is acting normally or under psychological manipulation
- Generates a **real-time intent risk score within milliseconds**, enabling adaptive safeguards without delaying legitimate transactions

Key Safety Interventions Enabled by the System

- Applies a **progressive transaction hold (30–120 seconds)** when high intent-risk is detected, preventing impulsive authorization while maintaining user control
- Activates **context-aware warning screens** that explicitly describe detected scam patterns (urgency, coercion, impersonation) instead of generic alerts
- Automatically surfaces a **trusted-contact verification panel**, allowing users to instantly call or message pre-selected contacts before proceeding
- Provides **one-tap escalation access** to official cybercrime helplines, bank fraud support, and in-app reporting channels
- Triggers **voice-based cognitive interruption alerts** (spoken warnings) to break panic-driven decision loops and restore rational attention
- Enforces **mandatory biometric re-authentication** for transactions flagged as high-risk, even if the user attempts repeated overrides
- Introduces a **secure last-step passkey / safety PIN**, requested **only during high-risk scenarios**, ensuring an additional conscious confirmation layer
- Implements **override throttling**, limiting repeated high-risk attempts within a short time window to prevent social-engineering pressure cycles

5. Why is this idea worth selecting? (Impact & value)

- Global digital payments exceed **hundreds of billions of transactions annually**, with real-time payment systems rapidly expanding across regions
- Worldwide financial fraud causes **over USD 1 trillion in losses every year**, with social engineering scams being the fastest-growing category
- Industry reports indicate that **60–70% of modern digital fraud incidents** succeed due to user manipulation rather than technical system failures
- Even a **5–10% reduction in social-engineering-driven fraud** can result in **tens of billions of dollars saved globally**
- Protects users **at the exact moment of decision-making**, where current systems have limited intervention capability
- Significantly reduces reliance on **post-transaction dispute and recovery processes**, which are costly and often ineffective

- Strengthens **global trust in real-time digital payment ecosystems**, a key requirement for financial inclusion and adoption
- Provides banks and fintech platforms with a **new behavioural intelligence layer** that complements existing fraud and AML systems
- Aligns with international regulatory priorities focused on **consumer protection, cybercrime prevention, and digital financial safety**

6. What is the USP (Unique Selling Proposition) of your idea?

- Treats **user intent as a first-class security signal**, going beyond transaction validity to understand *how and why* a payment is being made
- Uses **machine-learning–driven behavioural intelligence** by correlating interaction patterns, contextual signals, call activity, and location data in real time
- Introduces **progressive cognitive friction** (time delays, voice alerts, biometric re-checks, passkeys) instead of blunt transaction blocking
- Actively brings **human verification into the loop** through trusted contacts, cybercrime helplines, and bank support during high-risk moments
- Operates as a **pre-authorization safety layer**, intervening before irreversible actions occur
- Designed as a **plug-in security engine** that integrates seamlessly with existing banking, UPI, and real-time payment infrastructures
- Balances **strong fraud prevention with user experience**, minimizing false positives while maximizing protection
- Addresses a **currently unserved gap**: real-time intent inference during digital payment authorization