Building India's Intelligent Trust Layer



AI National Conference

20-Dec-25

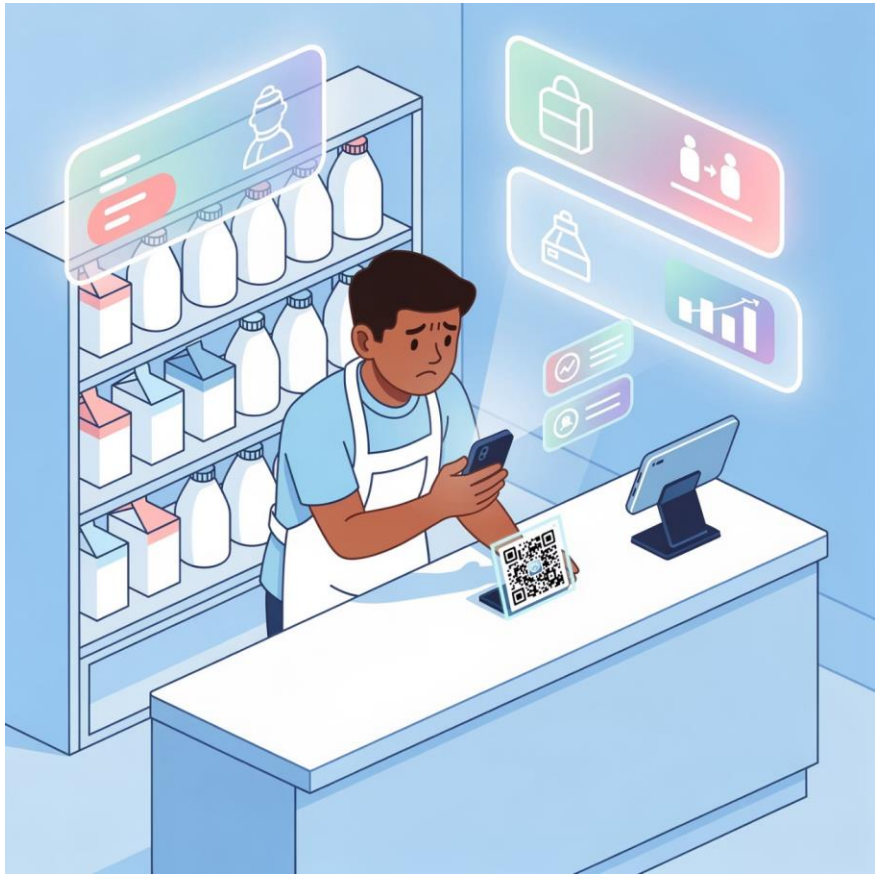
RS software

A QR Scam in Jaipur

Picture this: a small milk shop in Jaipur's old city. A polite customer arrives, scans the QR code on the counter, and shows a payment confirmation screen. The shopkeeper hands over the goods with a smile. But the payment never arrives.

The QR sticker was fake - printed overnight, pasted over the real one. The "confirmation" was a screenshot. By the time the shopkeeper realises what happened, the fraudster is three lanes away, repeating the trick at another kirana.

> **Fast money is brilliant. Fast fraud is devastating.**





The Core Tension

India Built the Fastest Payment Rails in the World

UPI processes transactions in seconds. Digital payments reach the remotest villages. Financial inclusion is no longer aspirational - it's operational reality.

Now We Must Build the Smartest Trust Layer

Speed without security is vulnerability at scale. Every innovation that delights customers also creates new attack vectors for fraudsters. The next decade demands intelligence, not just infrastructure.

Today's Agenda

01

India's Payments Revolution

Understanding the foundation, we've built

02

The New Threat Landscape

Real-time fraud in a real-time world

03

Why Fraud Must Be Real-Time

The 10-second problem

04

The Intelligent Trust Layer

Architecture for safety at scale

05

How AI Powers Protection

Machine learning meets fraud prevention

06

From Friction to Growth

Security as an enabler, not a barrier

07

India's Next Steps

Building the future together

India's Payments Revolution



UPI Everywhere

From metros to mandis, instant bank-to-bank transfers



QR-First Commerce

Zero-cost acceptance for millions of businesses



Aadhaar Integration

Biometric authentication enabling financial inclusion



FASTag Automation

Seamless toll payments across national highways



BBPS Standards

Unified bill payment rails for everyday services

The Numbers That Changed Everything

172B+

UPI Transactions

Processed in the last financial year alone

41–44%

Digital Payments CAGR

Explosive growth reshaping the economy





The Success Story

Digital Is No Longer Convenient. Digital Is the Default.

But There's a Dark Side

Real-Time Payments = Real-Time Fraud

Social Engineering

Impersonation of bank officials, delivery agents, or government authorities to trick users into sharing OTPs or credentials.

App Overlays and Screen Sharing

Malicious apps that mimic legitimate payment interfaces or remote access tools that allow fraudsters to control victim devices.

Fake QR Merchants

Counterfeit QR codes pasted over genuine ones, redirecting payments to fraudster accounts whilst displaying fake success screens.

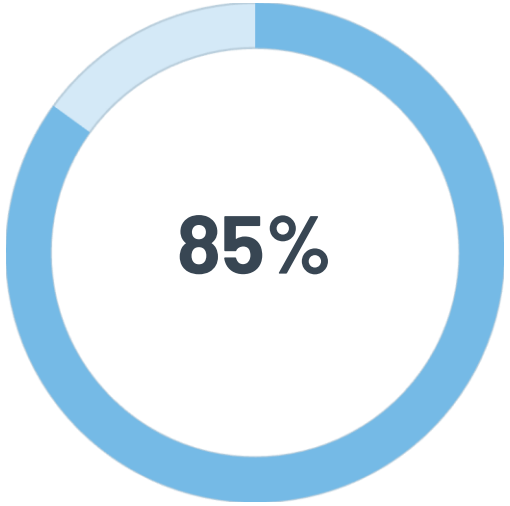
Mule Networks

Organised networks of compromised accounts used to move and layer stolen funds, making recovery nearly impossible.

OTP Compromise

Exploiting user trust to obtain one-time passwords through phishing, vishing, or malware-based interception.

The Scale of the Problem



Rise in UPI Fraud Complaints

Year-on-year increase reported to authorities



Losses from UPI Fraud

Reported losses, with true numbers likely higher



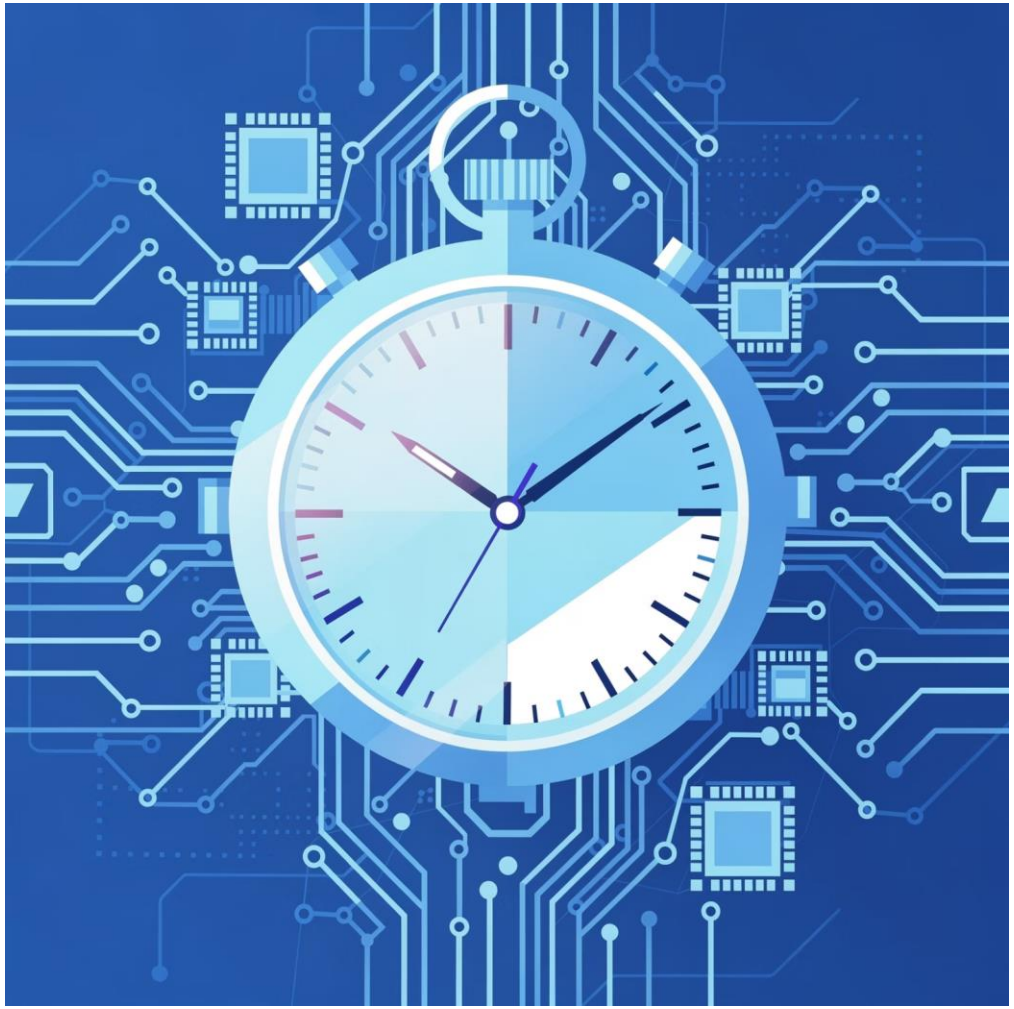
Card and Internet Banking Fraud

Additional losses across other digital channels

Why Fraud Must Be Detected in Real Time

The 10-Second Problem

1. **Transaction Initiated**
   User scans QR or enters UPI ID
2. **Funds Transferred (10 sec)**
   Payment completes, irreversible
3. **Layering Begins (2–5 min)**
   Funds moved through mule network
4. **Recovery Window Closes**
   Tracing becomes near impossible



Speed is the fraudster's greatest advantage.



What Real-Time Really Means

Millisecond Scoring

Risk evaluation must happen faster than the transaction itself

24×7 Data Streams

Continuous ingestion of behaviour, device, and network signals

Cross-Channel Visibility

Fraud doesn't respect silos—detection systems can't either

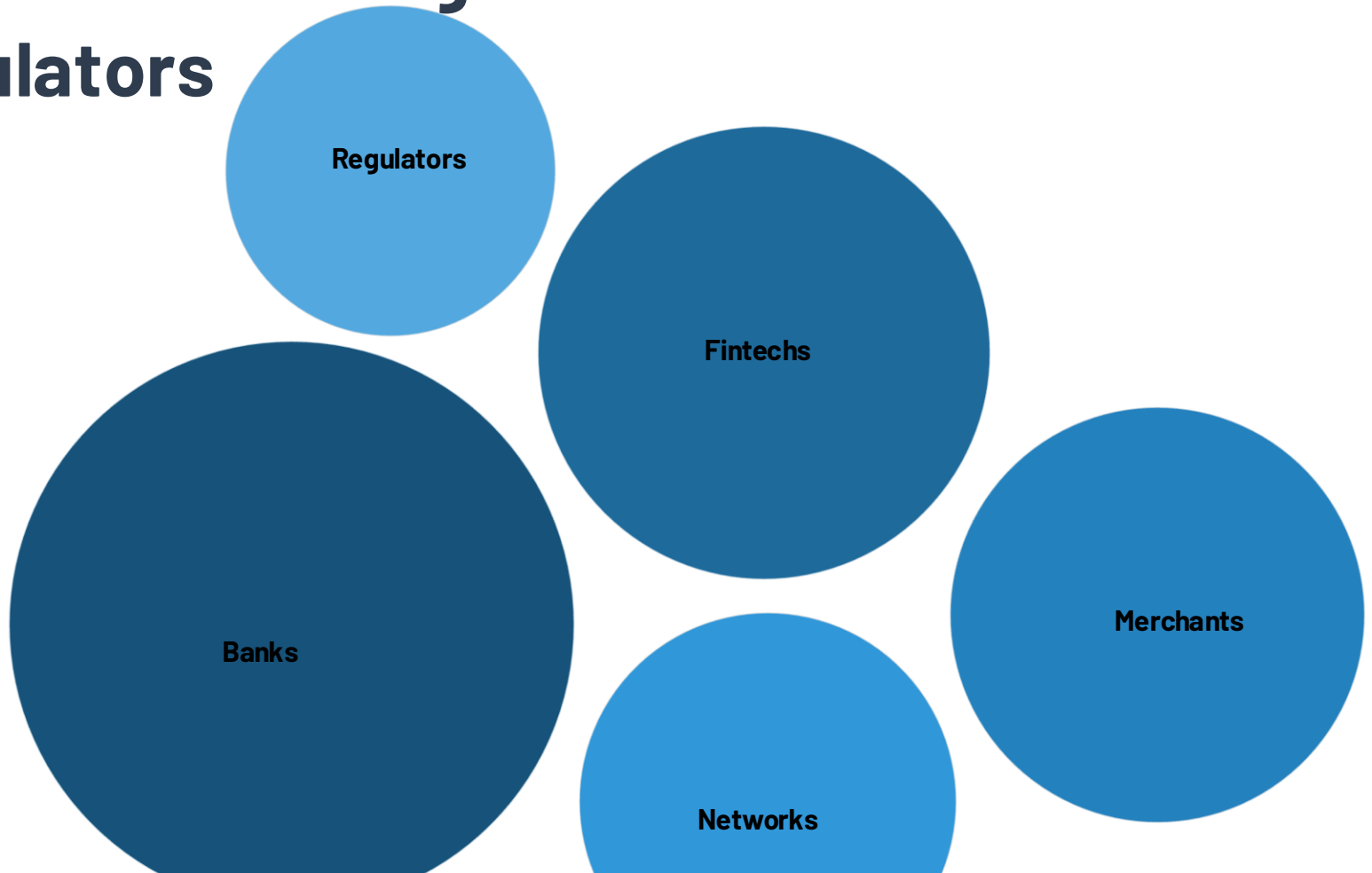
Continuous Learning

Models adapt as fraud tactics evolve, without manual intervention

What Is the Intelligent Trust Layer?

A horizontal safety net across the entire ecosystem

A unified platform connecting Banks • Fintechs • Merchants • Networks • Regulators





The Four Building Blocks

Unified Data Layer

Transactions, devices, identity, behaviour, and consortium signals in one place

Real-Time Decision Engine

Rules, ML, graphs, and context scoring every transaction instantly

Orchestration Layer

Dynamic actions from step-up auth to merchant controls

Feedback Loop

Continuous learning from fraud outcomes and analyst decisions

Unified Data Layer

Fraud hides in silos. Trust lives in shared signals.

Onboarding*

KYC data, Aadhaar linkage, face and fingerprints

Transactions

Amount, frequency, velocity, merchant category

Devices

Fingerprints, location, SIM changes, app integrity

Behaviour

Typical patterns, deviations, interaction history

Consortium Signals

Cross-institution fraud markers, mule account flags



*Onboarding fraud risk – 70%

Behavioural Biometrics

The invisible security layer

Monitoring 15 key behavioral signals in real-time allows for a robust, invisible layer of security.



Device Fingerprint



OS Type & Verification



Screen Size



Geo Location



Device Handling



In Active Call



Bot Activity



Navigation patterns



Click Speed



Typing Dynamics



Hand Eye Coordination



Date & Time patterns



Account Profile



Personal Profile



Personal/Business Profile

The "Profile Signals" (Hand Eye Coordination, Date & Time patterns, Account Profile, Personal Profile, Personal/Business Profile) are particularly important for detecting sophisticated fraud attempts.

Building User Profiles

Multi-dimensional behavioral analysis

Payer Profile - Multiple Dimensions

- Day of the Week
- Time of the Day
- Merchant Category Code
- Merchant Location
- Festive Season Variations
- Weather Impact
- Frequent Merchants

Payee Profile - High Frequency

- Day of the Week
- Time of the Day
- Brand/Reputation
- Average Ticket Size & Variability
- Cluster Average based on:
    - Location
    - Merchant Category Code
    - Festive Season

Needs Stream Analytics, Telescopic Summaries, Multi-D Aggregates and more

Challenge is Reading and Writing same information at Scale

Real-Time Decision Engine

Every transaction scored instantly

Rules

Hard limits, regulatory requirements, known fraud patterns

Machine Learning

Behaviour models, anomaly detection, predictive scoring

Graph Intelligence

Network analysis to detect mule accounts and layering patterns

Context

Time of day, location consistency, merchant reputation, user history



Graph analytics detect mule networks.

Rules, Models, or Hybrid?

Choosing the right approach

Rules

PROS: Explainable – Human Interpretable – Reuse Human Experience – Zero Day

CONS: Static – Difficult to Maintain

Maintenance: Regular review of rule efficacy and retiring of unproductive rules

Models

PROS: Dynamic

CONS: Explainability – Need Labelled Data (Takes Time to Build) – Drifts with Time

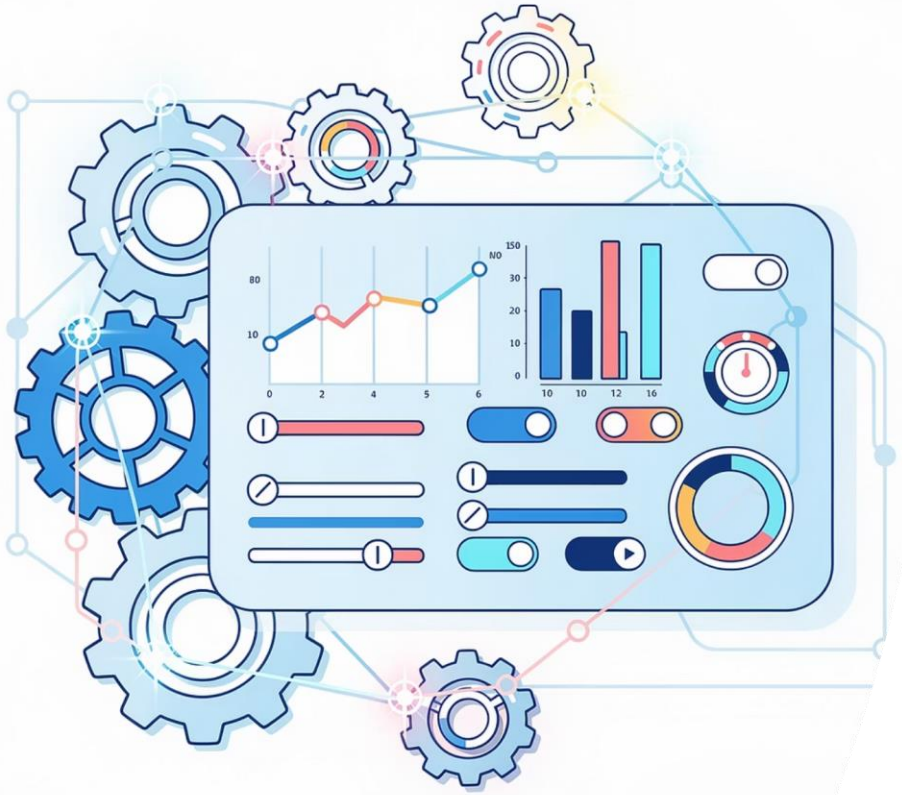
Maintenance: Build Shadow Models and replace when drift is detected

Hybrid ⭐

Structure by Human + Thresholds set by AI

Maintenance: Regular review of rule efficiency, build new thresholds in shadow

AI with Human-in-Loop is the right strategy as of now...



Orchestration Layer

Dynamic actions tailored to risk

Step-Up Authentication

Request additional verification for high-risk transactions

Transaction Holds

Temporary pause for manual review

Dynamic Limits

Adjust transaction or velocity limits based on behaviour

Real-Time Alerts

Notify users and analysts of suspicious activity

Merchant Risk Controls

Apply temporary restrictions to high-risk merchants

Automated Blocking

Immediate rejection of confirmed fraud patterns

Feedback Loop

The system never sleeps

The Intelligent Trust Layer is a dynamic system, constantly learning from every fraud outcome, analyst decision, and false positive to continuously retrain models and counter new attack patterns.

1. Fraud Outcomes

Confirmed fraud cases and false positives logged

2. Analyst Decisions

Human expertise captured and codified

3. Model Retraining

ML models updated with new patterns

4. Drift Detection

System monitors for model degradation

5. Pattern Recognition

New fraud tactics identified

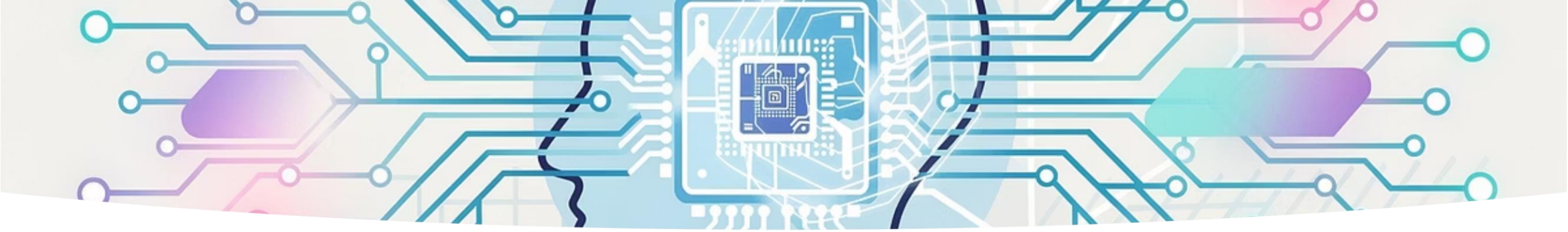
6. System Adaptation

Rules and models updated automatically





This continuous learning loop ensures our defenses evolve faster than any emerging threat.



How AI Makes This Possible

Artificial intelligence is crucial for fraud prevention, operating at the speed, scale, and sophistication required. India's leading fraud risk management systems achieve 99% accuracy in real-time fraud detection using AI-powered techniques.

Behaviour Modelling

Learning normal patterns for millions of users and detecting deviations instantly

Anomaly Detection

Identifying outliers that don't match any known fraud pattern but warrant investigation

Graph Intelligence

Mapping relationships between accounts, devices, and transactions to uncover fraud rings

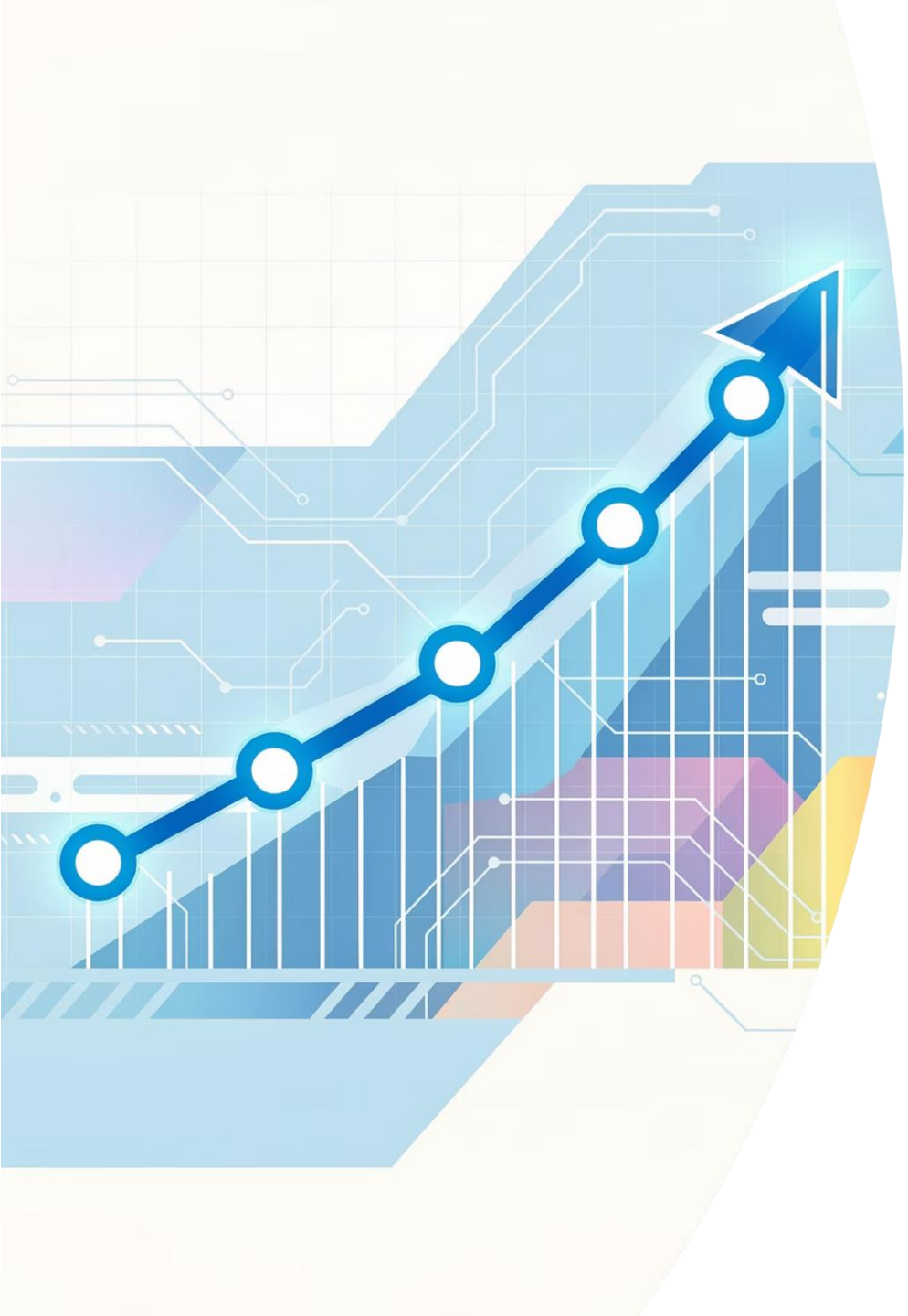
NLP on Scam Reports

Analysing customer complaints and social media to identify emerging fraud tactics

Model Lifecycle Tracking

Monitoring model performance, detecting drift, and triggering retraining automatically

Together, these AI techniques create a multi-layered defense, ensuring real-time adaptation, fewer false positives, faster approvals, and robust protection at scale.



From Friction to Growth

Security does not slow growth. Security allows growth.

Invisible AI-powered fraud prevention boosts customer experience, conversion, and adoption by instantly approving genuine transactions and minimizing false positives.

Reduces False Positives

Fewer legitimate transactions incorrectly flagged as fraud

Improves Approval Rates

More genuine customers complete transactions without friction

Lowers Cost Per Alert

Analysts focus on real threats, not noise

Boosts Merchant Trust

Businesses see fewer chargebacks and disputes

Supports RBI's Goals

Enables financial inclusion whilst maintaining system integrity

Trust embedded in the digital infrastructure benefits customers, merchants, and regulators, propelling India's payments ecosystem.

India's Next Steps

Building the future together

Realizing the full potential of the Intelligent Trust Layer requires coordinated action across the ecosystem from each stakeholder over the next five years.

Banks + Fintechs

Adopt AI-native fraud risk management platforms. Invest in real-time data infrastructure. Share consortium signals within regulatory frameworks.

Networks + Regulators

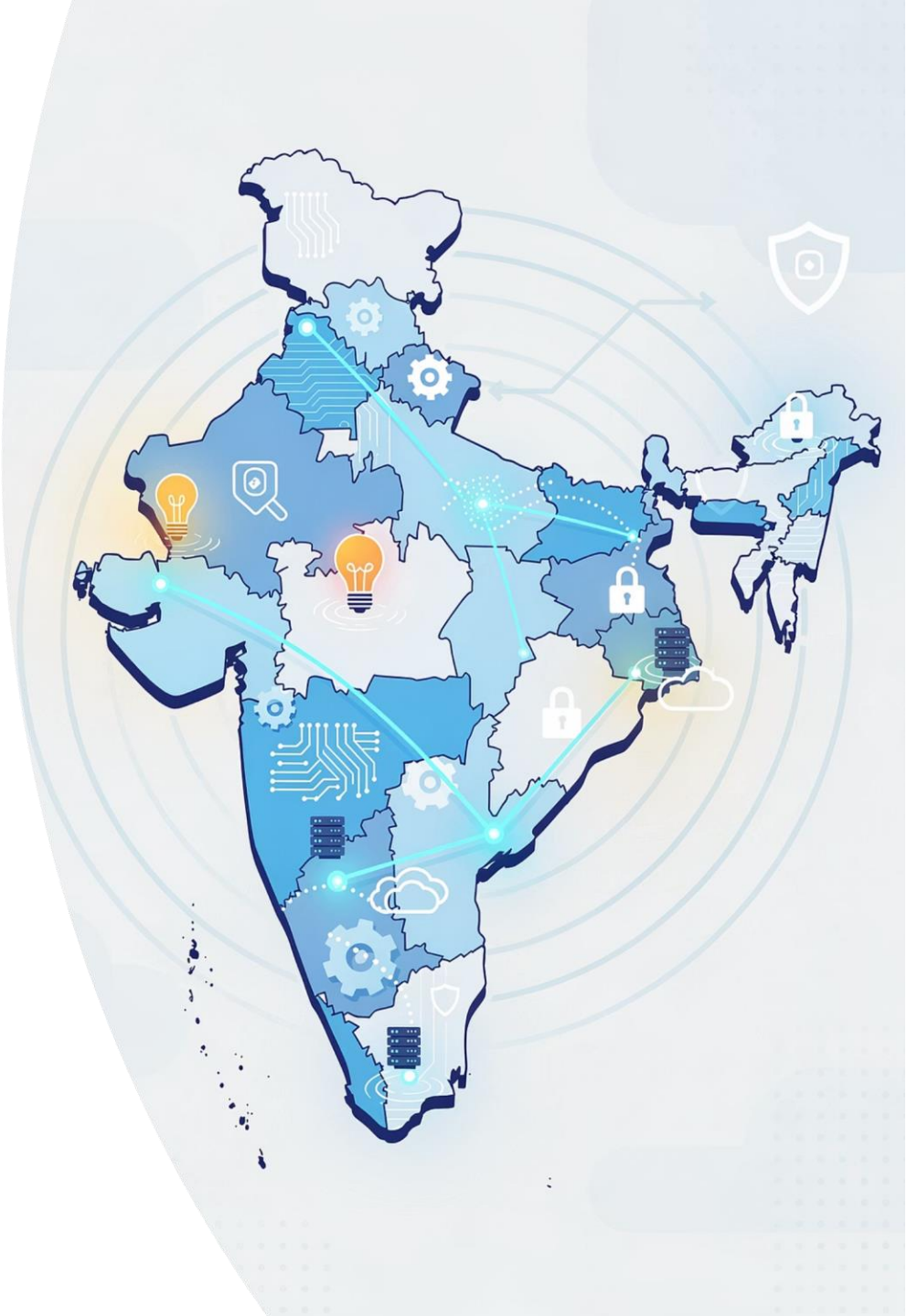
Enable secure data sharing standards. Establish interoperability protocols. Create incentives for ecosystem-wide fraud prevention.

Ecosystem Partners

Build awareness campaigns for merchants and consumers. Collaborate on fraud intelligence sharing. Develop training programs for fraud analysts.

The Country

Position India as the global model for trusted digital payments. Export learnings and technology to other markets. Lead the world in balancing innovation with security.



RS IntelliEdge™

Real-time protection at scale

Protecting the digital payments of India in Transacting Phase which includes rails like UPI, AEPS, IMPS, RuPay, FASTag, BBPS, and more.

20B+

Transactions Monthly

Across UPI, AEPS, IMPS, RuPay, FASTag, BBPS, and more

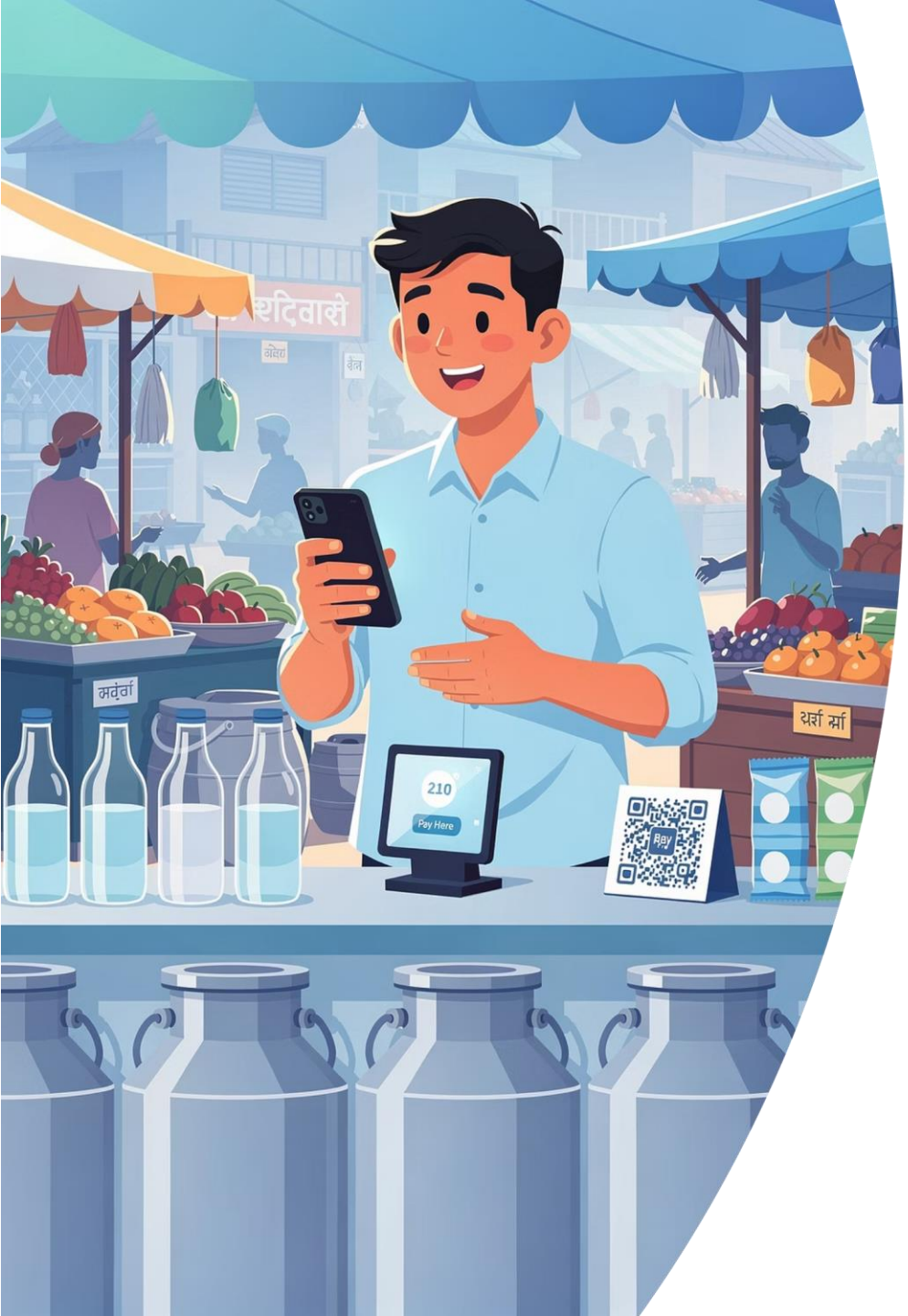
100ms

Average Latency

Ensuring near real-time protection across all rails

It has graph-based analytics engine to detect mule account and laundering activities almost in real time.





The Rails Are Built. Now Build the Trust.

The rails are built. Now India must build the trust layer that keeps them open, safe, and limitless.

- We started with a Jaipur milk shop story - a moment of misplaced trust repeated thousands of times daily.
- The infrastructure exists, technology is proven, and the ecosystem is ready.
- What remains is a commitment to collaboration and intelligence.
- India revolutionised payments. Now India will revolutionise trust.

> "Fast money is brilliant. Fast fraud is devastating. But intelligent trust? That's transformational."

Thank You



RS software