



Fraud Guardian

Priyanshi Goyal

Ameya Rathod

Dhananjay Goel

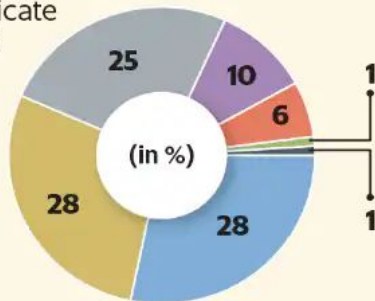
Devansh



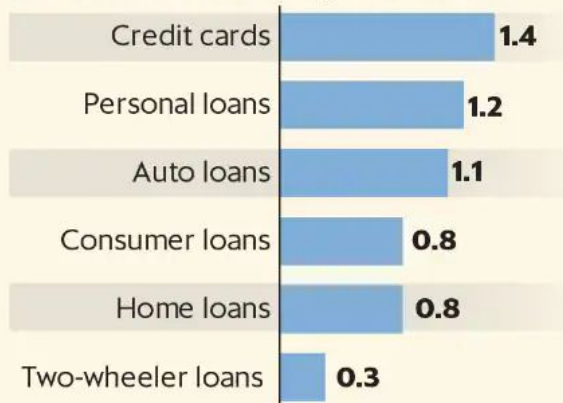
FRAUD TRENDS IN INDIA

As financial inclusion widens, frauds in the credit system increase. Delhi and West Bengal reported the highest month-wise incidences of fraud and credit cards emerged as the most vulnerable product

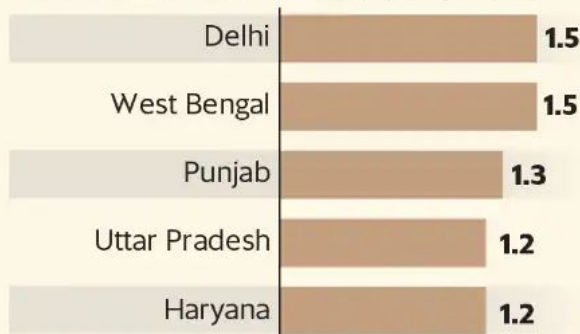
Distribution of different types of fraud in the credit system



Product-wise monthly fraud rates



Distribution of frauds by geography



*State-wise monthly fraud rates. Figures in %

Top reasons for declining applications for fraudulent intent

CREDIT CARDS



PERSONAL LOANS



Source: Experian India Fraud Report 2018-19

What's the problem?

- Fake payments, stolen cards, hacked accounts
- Looks like a normal transaction to the bank but it is not.
- £1 billion was stolen in 2024 in UK

TRANSACTION FRAUDS

- Fake IDs, morphed faces.
- System says verified - but it's a scam!
- Loan frauds by wrong KYC details.

Loan frauds

- Ponemon Institute 2023; Verizon and Gartner Reports show that significant portion of data breaches involve insiders

FRAUDS INVOLVING BANK EMPLOYEES/INSIDERS

Pain Points?

KYC - Manual Process

-Human intervention

Prevalent

Transaction - Classical

ML model

- not much explainability

Employee Behavior-

Not much existing

solutions

Transaction Frauds



Alex



Bob

Alex and Bob

SecureBank has a model trained on various transactions from its database that predicts if a transaction can be fraudulent or not.

The screenshot displays the ANZ New Zealand website. The top navigation bar includes the ANZ logo, a globe icon for 'New Zealand', and links for 'Join ANZ', 'Find a branch / ATM', 'Help', 'Contact us', and a search bar. Below this is a secondary menu with categories: 'Personal', 'Business', 'Institutional', 'Rural', 'About us', and 'Banking with ANZ'. The main content area is titled 'Help' and features a sidebar with links to various services: 'Accounts & everyday banking', 'Cards', 'Loans & overdrafts', 'Savings & investments', 'Foreign currency & travel', 'Online & phone banking', 'Branches & ATMs', 'Insurance', and 'Online meetings & chat'. The main content area is titled 'Search ANZ Help' and contains a search input field with the placeholder text 'Enter your question or keywords' and a 'Find' button. Below the search bar, the section 'Find transaction history - Internet Banking' is highlighted, with a sub-header 'How do I view my transaction history in ANZ Internet Banking?'. The text explains that users will arrive at a page showing their account balances and provides three ways to navigate to their transaction history: clicking 'View Recent transactions', clicking an account name, or clicking the 'Your accounts' tab. A screenshot of the ANZ Internet Banking interface is shown at the bottom, displaying a balance of \$43,549.89 and a 'Quick transfer' button.

Help

Accounts & everyday banking
Cards
Loans & overdrafts
Savings & investments
Foreign currency & travel
Online & phone banking
Branches & ATMs
Insurance
Online meetings & chat

Search ANZ Help

Enter your question or keywords **Find**

Find transaction history - Internet Banking
Last updated: 01 December 2020

How do I view my transaction history in ANZ Internet Banking?

When you log into ANZ Internet Banking you'll arrive at a page showing your account balances. There are three ways you can navigate to your account transaction history:

- Click the **View Recent transactions** link under the account you want to see transactions for. Scroll to the bottom of the transaction list and click **View Recent transactions** to go to the transaction history for that account
- Click on an account name from the accounts list and you'll be taken to a screen showing the transaction history for that account.
- Click on the **Your accounts** tab on the menu bar at the top of the page and select the account you want to see the transaction history for. You'll arrive at a screen showing the transaction history for the account you selected

You'll arrive at a screen showing the transaction history for the account you selected on the previous screen

ANZ ONLINECODE LOG OFF

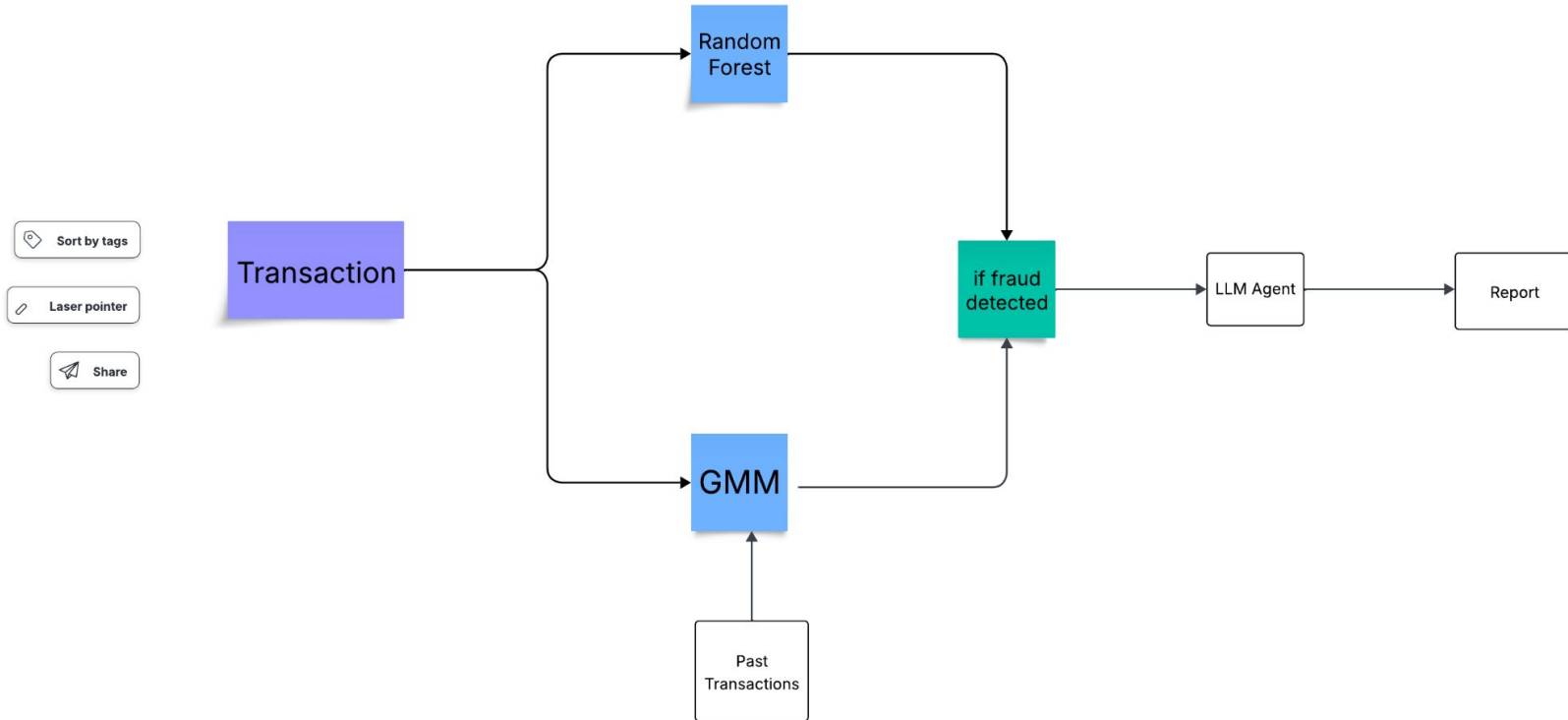
Home Your accounts Pay & transfer Apply & open Your settings Documents Bank mail

Go 00-0000-0099531-00 \$43,549.89 Available \$43,549.89 Quick transfer

Behaviour features

Number of clicks in the past hour, average time between clicks, session length, number of failed logins, device change rate, variance in location, actions performed per session.

Transactions Flowchart



SecureBank

Initiate a Transaction

Enter Transaction Details

To:

customer0

From:

Customer1

Time (YYYY-MM-DD HH:MM:SS):

2020-06-21 18:08:47

City Population:

128715

- +

Latitude:

43.232600

- +

Longitude:

-86.249200

- +

Amount (₹):

981.92

- +

Our USP

Transaction Based Detection

Involves monitoring customer transactions (money transfers, purchases, logins, etc.) to detect suspicious, abnormal, or unauthorized behavior that may indicate fraud

Employee Behaviour Analysis

Refers to analyzing internal staff behavior to detect potential insider threats, such as embezzlement, data leaks, or collusion with external fraudsters.

KYC Fraud Detection

Know Your Customer (KYC) is the process of verifying the identity of customers before/while doing business to prevent identity theft, money laundering, or fake account creation

Employee Behavior Analysis for Fraud Detection

Objective: Detect potential internal fraud or collusion within a bank using employee behavior analysis.

Approach:

- Monitor patterns like login/logout times, manual overrides, and failed login attempts.
- Use machine learning to assign a **fraud risk score** to each employee.
- Flag anomalies and trigger alerts for suspicious activity.
- Show the report made by GenAI to human reviewer for the reported frauds and retrain the model based on feedback.

Key Idea: Identify **deviations from normal behavior** that may signal insider threats.

ML-Based Risk Scoring Dashboard

- **Data Preprocessing:**

- Convert login/logout times to minutes.
- Derive work duration in minutes.
- One-hot encode employee roles.




- **Risk Prediction:**

- New CSV data scored in real-time.
- Risk Score (0-100) computed per employee.

- **Alerts & Visualization:**

- Trigger alerts based on thresholds (e.g., failed logins > 2).
- Visual dashboards: risk distribution, top risky employees, correlation heatmap.

Flowchart shapes

-  **Terminator**
Start and end points
-  **Process**
An action or function
-  **Decision**
A question to be answered
-  **Document**
The input/output of a document
-  **Data**
Data available for input/output

 Summarize


 Customize

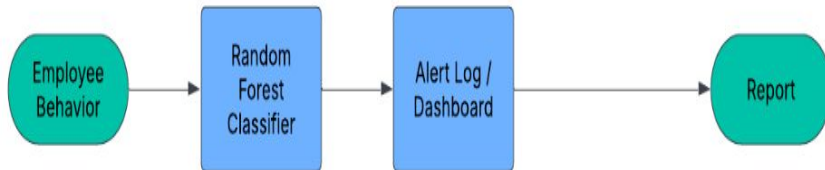
 Comment

 Share

Assisted layout container



Change any shape by selecting it and clicking the **Change shape** button. 



This container has assisted layout enabled to help structure the flowchart as it grows. Add shapes into the container to try it out!



Employee Fraud Risk Predictor & Dashboard

Upload the new employee data file (CSV)



Drag and drop file here

Limit 200MB per file • CSV

Browse files

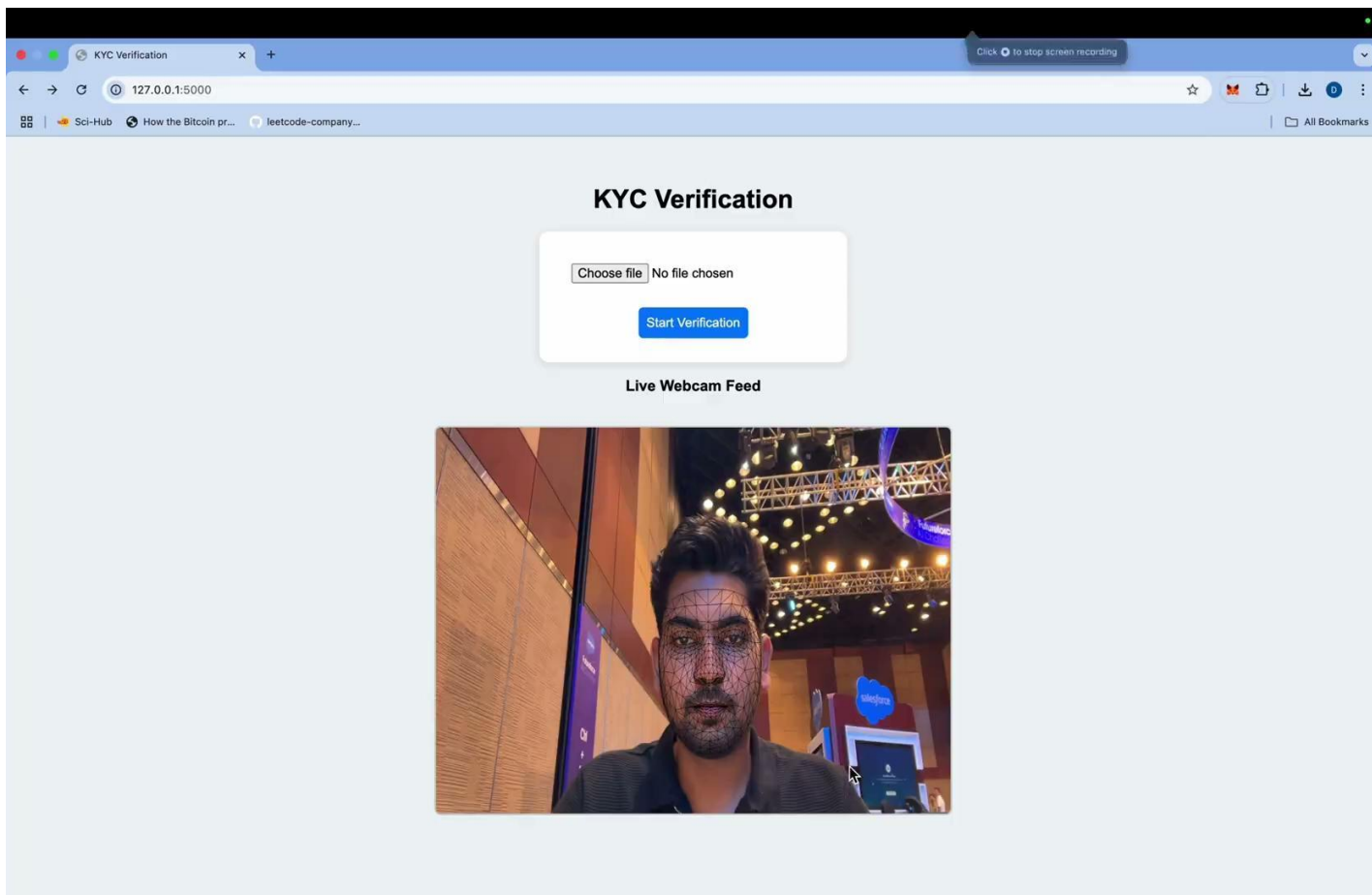
KYC Fraud Detection

Objective: Fraudsters increasingly use forged Aadhaar cards, deepfake videos, or static images during KYC

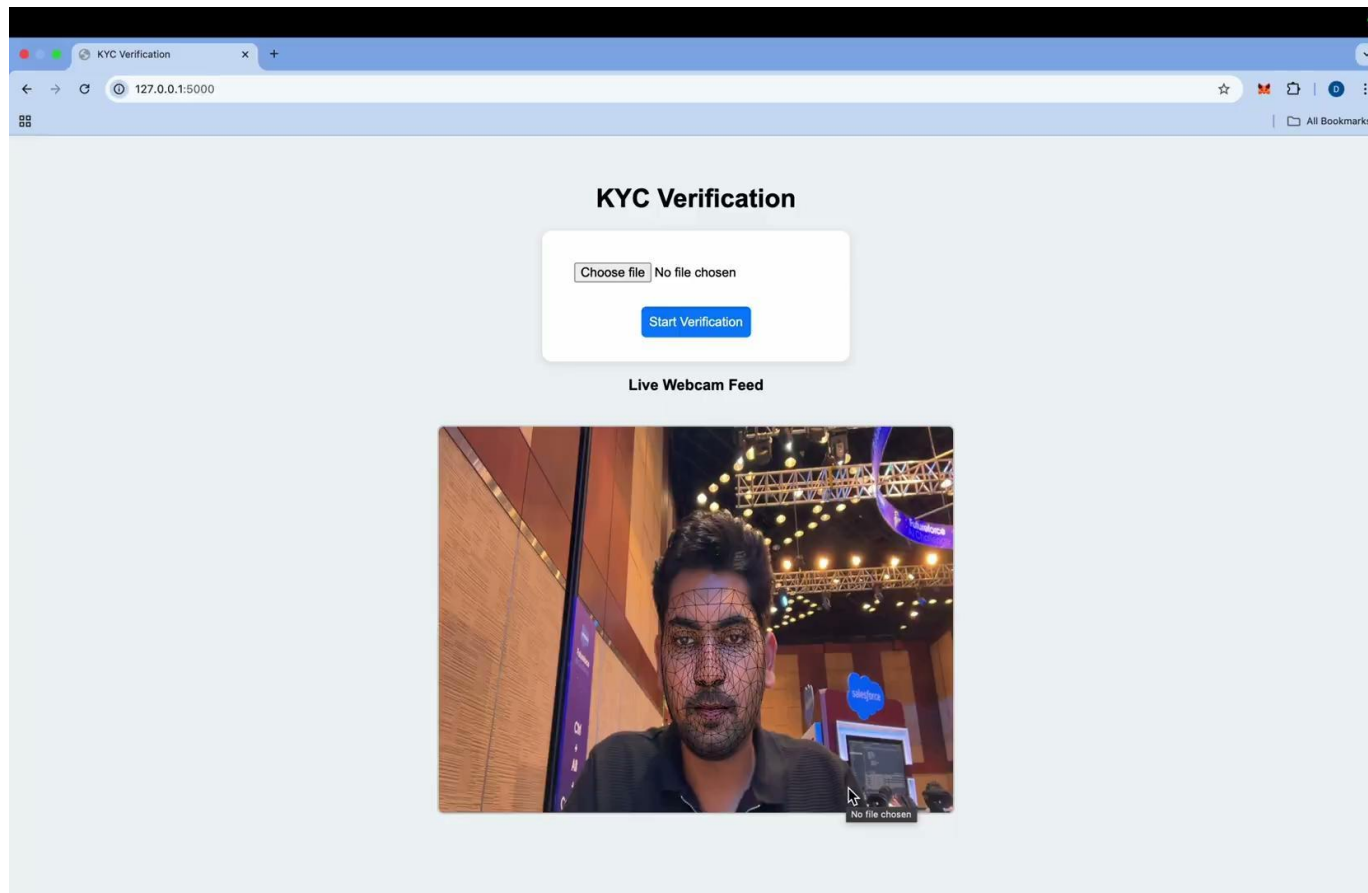
Approach:

- Real-time webcam feed with Face Mesh for accurate facial landmark detection
- Uses blinking detection to ensure the subject is live and not a photo/video
- Compares Aadhaar face with live webcam face to verify identity
- Integrated frontend and backend for seamless uploads, camera access, and real-time fraud prevention feedback.

Face Matching



Liveness Detection



Thank you