# Fraud Detection

# Table Of Contents

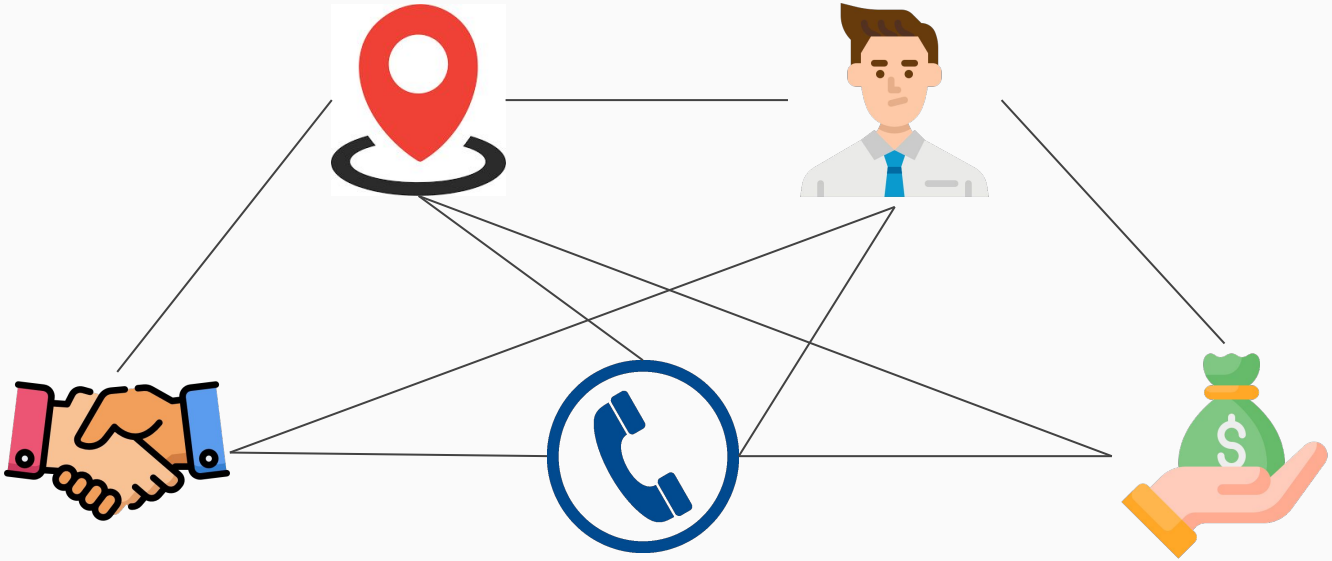
# Problem Statement

- **Selecting a fraud  from among thousands and doing a predictive performance analysis is a challenge which most of the bank's face.**
- **Evaluating fraudulent cases based on multiple attributes would not only help clients mitigate risk but also help reduce costs.**

Major issues arising in this area :

- **Disorganised information**
- **Banking data being disconnected due to privacy issues**
- **Solving in silos**

# User Story



# User Story

- Let’s say there was a hackathon at Microsoft Office!
- During the hackathon, some transactions occurred and **one of them** was **flagged** as fraudulent.
- We **flag** entire **office** on red-alert!
- This is part of entity - **address** :)

# Opportunity - Solutions

Channelize data points (by promoting open banking).

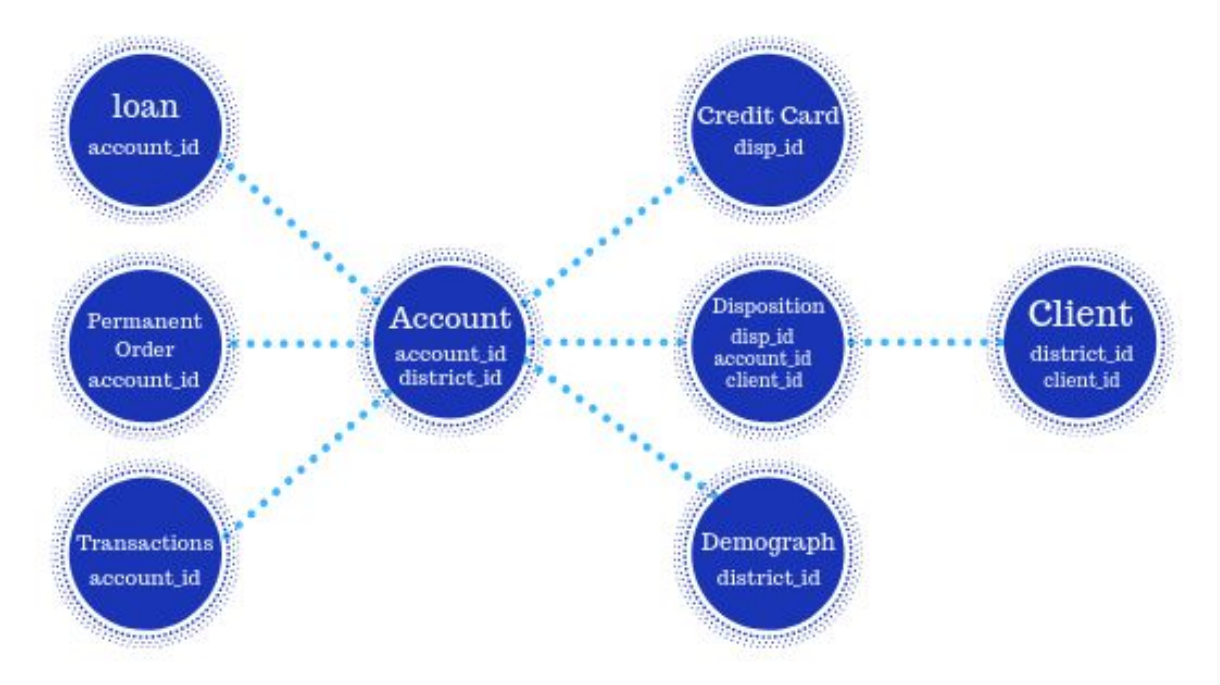
1. Understand patterns in account , transactions, order
2. Do entity resolution
3. Study parameters contributing the above through AI models
4. Zero knowledge proofing for transaction verification
5. ***Predict frauds.***

# Tech Stack and Libraries to be used

- Pandas
- Numpy
- Scikit Learn
- Blockchain - Python
- UI : Javascript, HTML,CSS

# Flowchart for AI MODEL

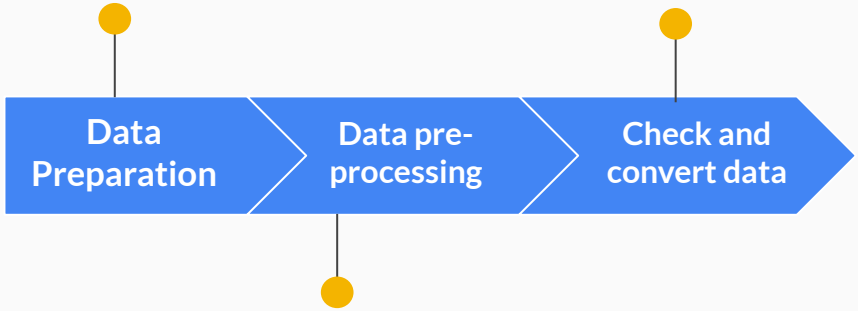
# Understanding the Data



# Data Preprocessing

Data Preparation Load, Clean and Format

Convert String values to categorical data

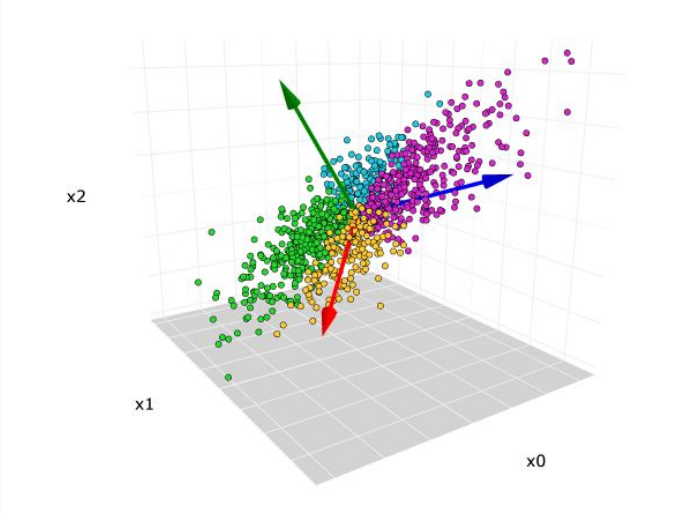



Missing values check

**Dataframes Used**

- orders
- transactions
- accounts

# Too Many Features? → Perform PCA!



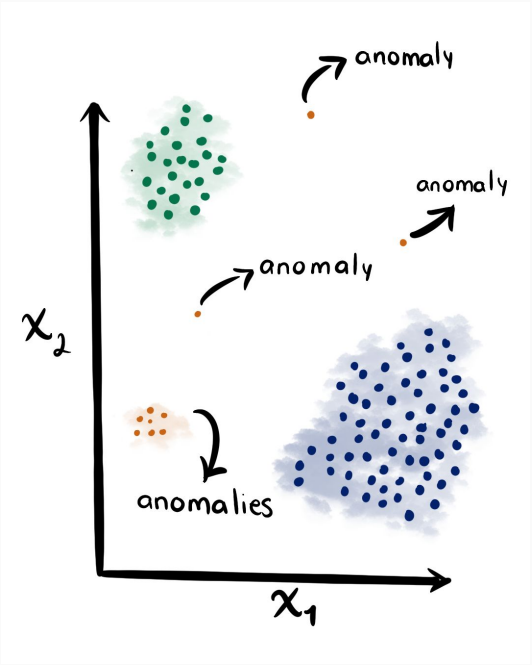

Reduce the dimension of the data from "36" to much lower. (tested with 2-5 components and compared variance.

# Anomaly Detection - K-Means with Outliers!

- Plot clusters with K-Means
- Calculate **distance** from each centroid
- Set threshold (>=0.8 distance)
- Label anomalies → “fraud”

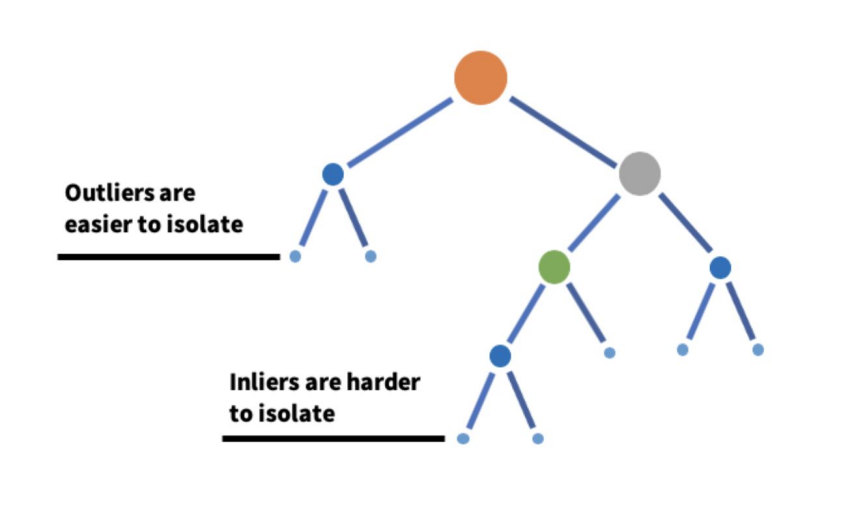
Another Approach:

- Size of cluster → too small?



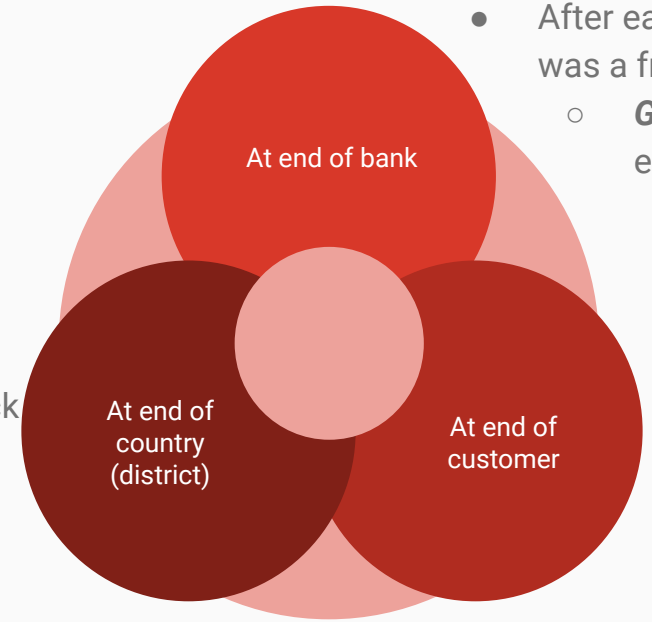
# Anomaly Detection - Isolation Forests!

- Create Random Forests based on the dataset
- Traverse entire tree after training
- Assign “anamoly_score” to each leaf node
- Detect anomalies according to the **threshold**



# Fraud Detection Pipeline

- After each **transaction** detect if it was a fraudulent transaction.
  - ***Generic and bigger*** frauds easily detected.




- In **regular interval** check for suspicious country transactions.
  - More hidden transactions.

- For each **customer** detect if after each transaction it was fraudulent.
  - Data obtained from a join with **disposition and client** csv.
  - K-means clusters would be more **personalized** and easier to detect fraud.

# UI Screens

FraudChurn

LOGIN SERVICES PORTFOLIO

## LOGIN

Choose according to your profile

### Entity

Resolve in Network

See Entity Resolution

Sign In

### Approver

Approve Contracts

Generate credits

Sign In

### Bank

Detect Frauds

Increase User Base

Sign In

## SERVICES

Logo

HOME | VIEW | SETTINGS | TRANSACTION VERIFICATION | LOGOUT

## APPLICATION DETAILS

Address : Hapur, UP West

Loans Applied : 2

Application Type: Education

Date : 12/2/2019

Account : xxx567900

Profession : Software Developer

Location : Hapur, UP West

Phone No. 1515151515

eyz@loan.com

☆ Credit Score ★ ★ ★

Looks fraudulent due to high amount money transactions done from Israel,China on same day

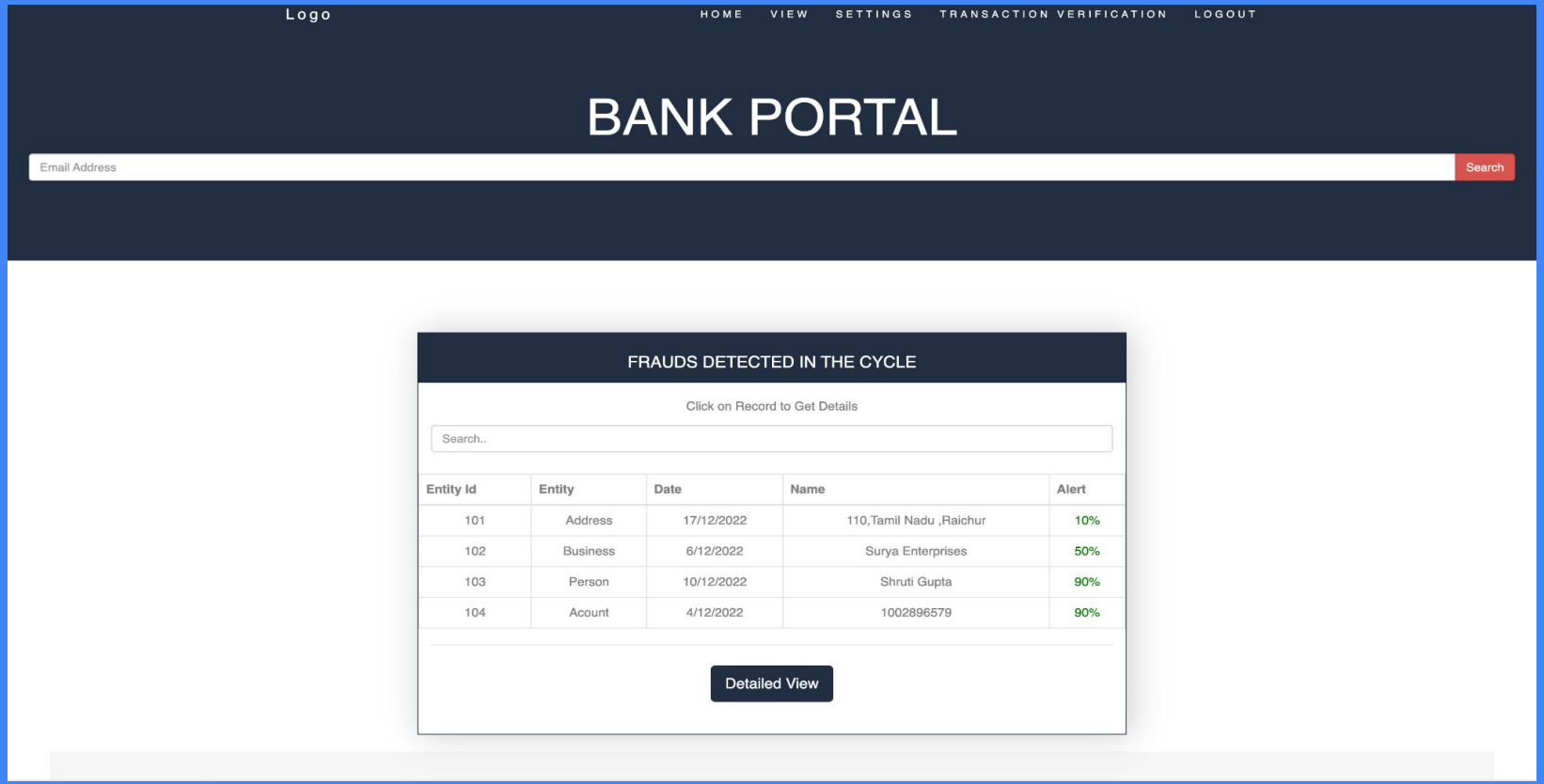
------ Miss Shruti Gupta ------

DOCUMENTS:

Document1

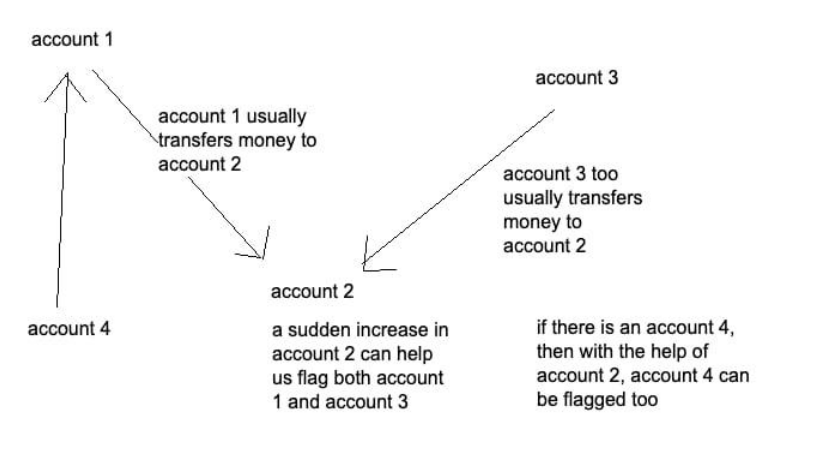
Aadhar Card

Send Notification | Block Account


Logo
HOME
VIEW
SETTINGS
TRANSACTION VERIFICATION
LOGOUT
BANK PORTAL
Email Address
Search
FRAUDS DETECTED IN THE CYCLE
Click on Record to Get Details
Search..
Entity Id
Entity
Date
Name
Alert
101
Address
17/12/2022
110,Tamil Nadu ,Raichur
10%
102
Business
6/12/2022
Surya Enterprises
50%
103
Person
10/12/2022
Shruti Gupta
90%
104
Acount
4/12/2022
1002896579
90%
Detailed View

# Future usage of Graph ML

Identifying  and establishing relationship among a different account created by same person.



# We aim to provide a complete solution..

- Entity Resolution
- ML Model

# Thank You!

# Solution

## Alert Creation for Fraud Prediction

- Recognize different entities in a system.
- Make a network.
- Create alerts on the network.
- Build a predictive model on transactions.
- Store transaction history on blockchain for feeding data to ML model
- **Online Learning:**
  - Real-time learning on new transaction
  - Batch training and feed to the ML model