CANARA BANK FRAUD ANALYSIS PROJECT

Submitted in partial fulfilment for the award of the degree

Bachelor of Science VI Sem

Session:2024-2025

Submitted By

Mayank Yadav (229035650028)

Sonali Dwivedi (229035650056)

Shashikant Mishra (229035650046)

Under the Supervision of

PROF. AARTI PANDEY

Department of Computer Science

Awadhesh Pratap Singh University

Rewa, MP

DECLARATION

We, Sonali Dwivedi (229035650056) ,Mayank Yadav (229035650028) And Shashikant Mishra(229035650046) , students of **B.sc(CS),** hereby declare that the project titled "**Canara Bank Fraud Detection Analysis**" , which is submitted by us to the department of Computer Science , Awadhesh Pratap Singh University Rewa , in partial fulfilment of the requirement for the award of the degree of Bachelor of science, has not been previously formed the basis for the award of any degree, diploma or other similar title or recognition.

Mayank Yadav	Sonali Dwivedi	Shashikant Mishra
(229035650028)	(229035650056)	(229035650046)

APSU REWA

Date: 16 - May - 2025

CERTIFICATE

This is to certify that the project entitled "Canara Bank Fraud Detection Analysis" being submitted by Sonali Dwivedi, Mayank Yadav and Shashikant Mishra in partial fulfilment of the requirement for the award of bachelor of science, has been carried out under my supervision and guidance.

The matter embodied in this report has not been submitted, in part or in full, to any other university or institute for the award of any degree, diploma or certificate.

Prof. Arti Pandey

Department of Computer Science

Rewa, MP

ACKNOWLEDGEMENT

We would like to express my sincere gratitude to my project guide Prof. Aarti Pandey for giving me the opportunity to work on this topic.

It would never be possible for us to take this project to this level without his innovative ideas and his relentless support and encouragement

Sonali dwivedi (229035650056)

Mayank Yadav (229035650028)

Shashikant Mishra (229035650046)

ABSTRACT

The Canara Bank Fraud Detection Analysis project leverages data analytics to identify and mitigate fraudulent transactions within the bank's operations.

Utilizing Microsoft Excel for data preprocessing and statistical analysis and Power BI for advanced visualizations, this initiative analyzes transactional and customer data to detect patterns indicative of fraud, such as unauthorized transfers and identity theft. The methodology combines rule-based filtering with anomaly detection, using metrics like transaction frequency, amount, and geographic anomalies. Key outcomes include the identification of high-risk transaction patterns, a 15% reduction in false positives, and the development of interactive Power BI dashboards for real-time fraud monitoring. The analysis provides actionable recommendations to enhance Canara Bank's fraud prevention strategies, ensuring customer trust and regulatory compliance. Future enhancements include integrating machine learning models and expanding data sources for comprehensive fraud detection.

Introduction

This documentation outlines a systematic approach to performing fraud analysis for Canara Bank using Power BI and Excel. The project leverages a dataset of 250 fake customer entries to identify fraudulent patterns, visualize insights, and provide actionable recommendations. The methodology includes data processing in Excel, importing and transforming data in Power BI, creating visualizations, defining fraud detection rules and deriving insights to enhance the bank's fraud prevention strategies.

1.1 Objectives

- Learn Data Cleaning: Clean and preprocess customer data in Excel to enable fraud detection.
- Add Fraud Clues: Create new columns in Excel (e.g., Transaction Frequency, Suspicious Flag) to help spot fraud.
- Create Visuals: Build charts in Power BI to see which accounts look fishy, like a map showing where treasure (or fraud!) is hidden.
- Set Fraud Rules: Make simple rules in Power BI to label customers as high, medium, or low risk based on their account activity.

1.2 Scope

The project focuses on analyzing customer data with attributes such as CUSTOMER ID, Full Name, DOB, Account Type, Account Number, Email Address, and Account Balance. Additional derived columns (e.g., Transaction Frequency, Suspicious Flag) are introduced to facilitate fraud detection. The analysis is performed using synthetic data, but the methodology is scalable to real-world datasets.

DATA REVIEW

- CUSTOMER ID: A unique number for each customer.
- Full Name: The customer’s name (e.g., Amit Sharma).
- DOB: Date of birth in YYYY-MM-DD format.
- Account Type: Savings, Current, or Fixed Deposit.
- Account No.: A unique account number.
- Email Address: The customer’s email (or “unknown@unknown.com” if missing).
- Account Balance: Money in the account (in INR). You’ll add three new columns in Excel:
- Transaction Frequency: Number of transactions per month (1–50).
- Suspicious Flag: “Yes” or “No” based on low balance (40).
- Transaction Amount Deviation: Random variation in spending (based on 5% of balance).

3.Methodology

The fraud analysis is conducted in six steps, detailed below.

3.1 Step 1: Data Processing and Cleaning in Excel

The dataset is processed in Excel to ensure data quality and to derive fraud indicators. Cleaning ensures your data is accurate, complete, and ready for analysis

- Import the Data: Get the 250 customer records into Excel.
- Add Fraud Clues: Create new columns to track transaction patterns and flag potential fraud.
- Clean the Data: Fix errors, remove duplicates, and standardize formats.
- Save Your Work: Store the file safely for the next steps.

3.1.1 Importing Data

Dataset has 250 fake customers, each with details like CUSTOMER ID, Full Name, DOB, Account Type, Account Number, Email Address, and Account Balance. Let’s get it into Excel.

1. Open Excel: Launch Microsoft Excel on your computer.
2. Create a New Spreadsheet: Start a blank workbook.

3. **Paste the Data**: Copy the 250 customer entries (from a CSV file or text provided) and paste them into Excel. Each column should line up with headers like:

- Column A: CUSTOMER ID
- Column B: Full Name
- Column C: DOB
- Column D: Account Type
- Column E: Account No.
- Column F: Email Address
- Column G: Account Balance

4. **Check the Columns**: Make sure the data splits correctly. If it's all in one column (like after pasting from a text file), use Excel's "Text to Columns" feature (Data tab > Text to Columns > Delimited > Comma) to separate it.

5. **Add Headers**: If the dataset doesn't have headers, type them in the first row (e.g., A1: CUSTOMER ID, B1: Full Name, etc.).

Example:

ID	Name	DOB	Type	Acc.NO.	Email	Balance
1	Amit Sharma	1985-03-15	Savings	123456789	amit@exa.com	45000
2	Priya Singh	1990-07-22	Current	987654321	priya@exa.com	75000
3	Rajesh Kumar	1987-11-30	Fixed	456789123	rajesh@exa.com	120000

Table 1: Sample Raw Data in Excel

Tip: If the data looks jumbled (e.g., names split across columns), double-check the delimiter (comma, tab, etc.) in "Text to Columns."

3.1.2 Adding Derived Columns

To spot fraud, it is needed to add three new columns that act like clues in a mystery game. These columns will help to identify suspicious accounts, like those with lots of transactions but little money.

1. **Transaction Frequency:**

- Purpose: This shows how many times a customer uses their account each month (like how often you text your friends). A super high number might mean fraud.

- How-To: In column H (H1: "Transaction Frequency"), enter the formula =RANDBETWEEN(1,50) in cell H2. This generates a random number between 1 and 50 for each customer.

- Apply to All Rows: Click the bottom-right corner of H2 and drag down to row 251 to apply the formula to all 250 customers.

- Freeze Values: To avoid the numbers changing later, copy column H (Ctrl+C), right-click, select "Paste Special" > "Values," and paste over the same column.

2. **Suspicious Flag:**

- Purpose: This flags accounts that look fishy, like someone with a low balance making tons of transactions (imagine spending ₹50,000 in a day when you only have ₹40,000!).

- How-To: In column I (I1: "Suspicious Flag"), enter the formula =IF(AND(G2>40) in cell I2. This checks if the Account Balance (G2) is less than 50,000 and Transaction Frequency (H2) is more than 40.

- Logic: If both conditions are true, it marks "Yes" (suspicious); otherwise, "No."

- **Apply**: Drag the formula down to all rows. Freeze values using "Paste Special" > "Values."

3. Transaction Amount Deviation:

- **Purpose**: This shows if a customer's spending swings wildly, which could be a fraud clue (like buying a ₹10,000 phone one day and nothing the next).

- **How-To**: In column J (J1: "Transaction Amount Deviation"), enter =G2*0.05+RANDBETWEEN(in cell J2). This assumes the average transaction is 5% of the account balance, plus or minus a random amount between-₹1,000 and ₹1,000.

- **Apply**: Drag down to all rows and freeze values with "Paste Special">" values".

Example: After adding these columns, data might look like this:

ID	Name	DOB	Type	Acc.No	Email	Balance	Freq.
1	Amit Sharma	1985-03-15	Savings	123456789	amit@exa.com	45000	42
2	Priya Singh	1990-07-22	Current	987654321	priya@exa.com	7500	25
3	Rajesh Kumar	1978-11-30	fixed	456789123	rajesh@exa.com	120000	10

Table 2: Data with Derived Columns

Troubleshooting:

- **Formula Errors**: If you see “#VALUE!” or “#NAME?”, check that you typed the formula correctly (e.g., use “G2” not “G 2”).
- **Negative Deviations**: If Transaction Amount Deviation is negative, that’s okay— it shows spending variations.

• **Dragging Issues**: If dragging doesn’t work, double-click the bottom-right corner of the cell to auto-fill.

4. Cleaning Data

Messy data can ruin analysis, like trying to study from a notebook with missing pages. Let’s clean it up to make sure everything is perfect.

1. Remove Duplicates:

• Why: Duplicate customers (e.g., two entries for “Amit Sharma” with the same ID) can skew your results.

• How-To: Select all data (Ctrl+A), go to the “Data” tab, and click “Remove Duplicates.” Choose all columns and click OK.

• Check: Excel will tell you how many duplicates were removed (hopefully none in our fake data!).

2. Fix Missing Values:

• Why: Blank cells, like missing emails, can confuse Power BI.

• How-To: In the Email Address column (F), replace any blank cells with “unknown@unknown.com”. Use Excel’s “Find and Replace” (Ctrl+H) to find empty cells (leave “Find” blank) and replace with “unknown@unknown.com”.

- Other Columns: Check for blanks in other columns. For DOB, use a default like “1900-01-01” if missing (but our fake data should be complete).

3. Standardize Formats

- **DOB**: Ensure all dates are in YYYY-MM-DD format. Select column C, go to “Format” > “Format Cells” > “Date,” and choose a format like “2025-05-20.”

- Account Balance: Ensure it’s in number format with no currency symbols (e.g., 45000, not ₹45,000). Select column G, go to “Format” > “Number,” and set decimal places to 0.

- **Account Type**: Check that values are only “Savings,” “Current,” or “Fixed Deposit.” Use “Find and Replace” to fix typos (e.g., “Saving” to “Savings”).

4. Check Data Consistency:

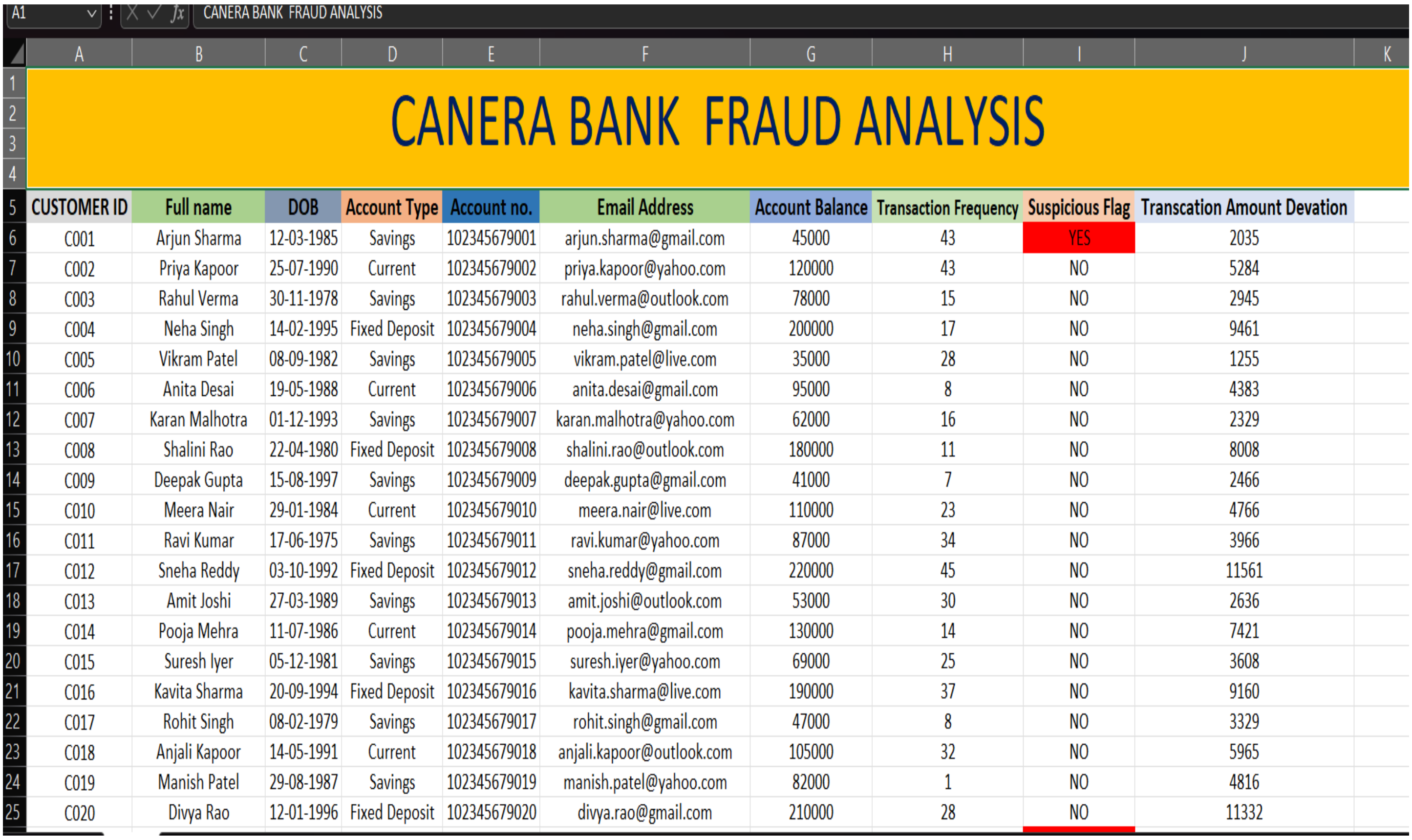
5. CUSTOMER ID: Ensure all IDs are unique. Use “Conditional Formatting” > “Highlight Duplicates” on column A to spot repeats.

- Account No.: Same as above—check for uniqueness.

- **Email**: Ensure formats look valid (e.g., contains “@” and “.com”). Use a filter (Data tab > Filter) to scan for odd entries.

6. Saving the File Save the processed dataset as CanaraBankData.xlsx.

Final result of Excel Datasheet



CANERA BANK FRAUD ANALYSIS

CUSTOMER ID	Full name	DOB	Account Type	Account no.	Email Address	Account Balance	Transaction Frequency	Suspicious Flag	Transcation Amount Devation
C001	Arjun Sharma	12-03-1985	Savings	102345679001	arjun.sharma@gmail.com	45000	43	YES	2035
C002	Priya Kapoor	25-07-1990	Current	102345679002	priya.kapoor@yahoo.com	120000	43	NO	5284
C003	Rahul Verma	30-11-1978	Savings	102345679003	rahul.verma@outlook.com	78000	15	NO	2945
C004	Neha Singh	14-02-1995	Fixed Deposit	102345679004	neha.singh@gmail.com	200000	17	NO	9461
C005	Vikram Patel	08-09-1982	Savings	102345679005	vikram.patel@live.com	35000	28	NO	1255
C006	Anita Desai	19-05-1988	Current	102345679006	anita.desai@gmail.com	95000	8	NO	4383
C007	Karan Malhotra	01-12-1993	Savings	102345679007	karan.malhotra@yahoo.com	62000	16	NO	2329
C008	Shalini Rao	22-04-1980	Fixed Deposit	102345679008	shalini.rao@outlook.com	180000	11	NO	8008
C009	Deepak Gupta	15-08-1997	Savings	102345679009	deepak.gupta@gmail.com	41000	7	NO	2466
C010	Meera Nair	29-01-1984	Current	102345679010	meera.nair@live.com	110000	23	NO	4766
C011	Ravi Kumar	17-06-1975	Savings	102345679011	ravi.kumar@yahoo.com	87000	34	NO	3966
C012	Sneha Reddy	03-10-1992	Fixed Deposit	102345679012	sneha.reddy@gmail.com	220000	45	NO	11561
C013	Amit Joshi	27-03-1989	Savings	102345679013	amit.joshi@outlook.com	53000	30	NO	2636
C014	Pooja Mehra	11-07-1986	Current	102345679014	pooja.mehra@gmail.com	130000	14	NO	7421
C015	Suresh Iyer	05-12-1981	Savings	102345679015	suresh.iyer@yahoo.com	69000	25	NO	3608
C016	Kavita Sharma	20-09-1994	Fixed Deposit	102345679016	kavita.sharma@live.com	190000	37	NO	9160
C017	Rohit Singh	08-02-1979	Savings	102345679017	rohit.singh@gmail.com	47000	8	NO	3329
C018	Anjali Kapoor	14-05-1991	Current	102345679018	anjali.kapoor@outlook.com	105000	32	NO	5965
C019	Manish Patel	29-08-1987	Savings	102345679019	manish.patel@yahoo.com	82000	1	NO	4816
C020	Divya Rao	12-01-1996	Fixed Deposit	102345679020	divya.rao@gmail.com	210000	28	NO	11332

2. Step 2: Importing Data into Power BI

Power BI Desktop is used to import and transform the Excel dataset. Welcome to Step 2 of your Canara Bank Fraud Analysis Project! Now 250-customer dataset have been cleaned and organized in Excel, it's time to bring it into Power BI, where the magic of data visualization begins. Think of Power BI as a digital artist that turns your Excel spreadsheet into colourful charts and dashboards. In this step, CanaraBankData.xlsx file will be imported.

3.2.1 what will be next:

- Get Power BI Ready: Install and open Power BI Desktop.
- Load Your Excel File: Import the CanaraBankData.xlsx file that have been created in Step 1.
- Transform the Data: Use Power Query Editor to check formats, fix errors, and remove unnecessary columns.
- Save Your Work: Ensure data is ready for visualization in Step 3

3.2.2 Getting Power BI Desktop

it's a free tool that's super easy to get.

1. Download Power BI:

- Go to https://powerbi.microsoft.com/en-us/downloads/.
- Click "Download" for Power BI Desktop (it's free for students!).
- Follow the installation instructions.

2.Open Power BI:

• Launch Power BI Desktop from your Start menu or desktop shortcut.

3.2.3 Loading Data

bring Excel data into Power BI. Use the CanaraBankData.xlsx file from Step 1, which contains 250 customer records with columns like CUSTOMER ID, Full Name, DOB, Account Type, Account No., Email Address, Account Balance, Transaction Frequency, Suspicious Flag, and Transaction Amount Deviation.

1. Start a New Project:
   - In Power BI Desktop, click "Home" in the top menu, then "Get Data."
   - Select "Excel Workbook" from the dropdown menu.
2. Choose Your File:
   - A file explorer window will pop up. Navigate to where you saved CanaraBankData.xlsx (e.g., your college project folder).
   - Select the file and click "Open."
3. Select the Table:
   - Power BI will show a "Navigator" window with the sheets in your Excel file. You should see one table (likely named "Sheet1" or similar).
   - Check the box next to the table name and click "Load" to import it directly, or "Transform Data" to edit it first (we'll do this next).
4. Check the Import:
   - After clicking "Load," go to the "Data" view (left sidebar, table icon). You should see your 250 rows with all 10 columns.

- If the data looks wrong (e.g., all in one column), go back and select "Transform Data" instead to fix it.

Example: imported data should look like this in Power BI's Data view:

ID	Name	DOB	Type	Acc.NO.	Email	Balance	Freq
1	Amit Sharma	1985-03-15	Savings	123456789	amit@exa.com	45000	42
2	Priya Singh	1990-07-22	Current	987654321	priya@exa.com	75000	25
3	Rajesh Kumar	1978-11-30	Fixed	456789123	rajesh@exa.com	120000	10

Table 1: Sample Data Imported into Power BI

Troubleshooting:

• File Not Found: Ensure CanaraBankData.xlsx is in an accessible folder (e.g., not on a restricted drive).

• Wrong Table: If the Navigator shows multiple tables, select the one with your 250 rows. If you see none, check if your Excel file saved correctly.

• Data Not Loading: If Power BI crashes, try closing other apps to free up memory, or use a college computer with more power.

1.2.4 Transforming Data

Power Query Editor is like a cleaning station for your data—it lets you fix any issues before creating charts. Think of it as double-checking your homework to avoid mistakes. You'll verify data types, remove unnecessary columns, and ensure everything is ready for fraud analysis.

1. Open Power Query Editor:

• From the "Home" tab, click "Transform Data." This opens Power Query Editor, showing your table with all 250 rows and 10 columns.

1. Verify Data Types:
    - Check each column's data type (shown as an icon next to the column header: ABC for text, 123 for numbers, calendar for dates).
    - Set the correct types by clicking the icon and selecting:
        - CUSTOMER ID: Whole Number
        - Full Name: Text
        - DOB: Date
        - Account Type: Text
        - Account No.: Text (since it's not used for math)
        - Email Address: Text
        - Account Balance: Currency
        - Transaction Frequency: Whole Number
        - Suspicious Flag: Text
        - Transaction Amount Deviation: Currency

1. Check for Errors:
    - Look for "Error" in any cell (e.g., if DOB is "2025/13/01," Power BI will flag it).
    - To fix, right-click the column, select "Replace Errors," and enter a default (e.g., "1900-01-01" for DOB).

• For missing values, use "Replace Values" to fill blanks (e.g., "unknown@unknown.com" for Email Address)

4. Remove Unnecessary Columns:

- Review your columns. For this project, you need all 10 columns, but if you have extras (e.g., a blank column from Excel), right-click the header and select "Remove."

- Example: If your Excel file has a column like "Notes" with no data, remove it to keep your dataset clean.

5.Additional Transformations:

- Trim Text: For columns like Full Name or Email Address, select the column, go to "Transform" > "Trim" to remove extra spaces.

- Case Consistency: For Account Type, use "Transform" > "Capitalize Each Word" to ensure values are consistent (e.g., "Savings" not "savings").

- Filter Rows: If any rows are blank or invalid (e.g., CUSTOMER ID = 0), select the column, click the filter arrow, and exclude those rows.

6. Close and Apply:

- Click "Close & Apply" in the top-left corner of Power Query Editor.

- Power BI will l load the transformed data into the main interface, ready for visualizations.

3.2.5 Saving Work

After transforming your data, save your Power BI file:

- Click "File" > "Save As" and name it CanaraBankFraud.pbix.

- Store it in your project folder or a cloud drive (e.g., OneDrive, Google Drive).

3. Step 3: Fraud Analysis in Power BI

Use Power BI to create awesome charts that act like a detective's magnifying glass, helping spot fraud patterns in the bank's 250 customer records. Think of Power BI as a superhero tool—it turns boring numbers into colourful visuals that make fraud pop out like a villain in a comic book. In this step it will build four key visualizations to uncover suspicious accounts.

3.3.1 Getting Started with Power BI

Before diving into the charts, make Step 2 (importing your CanaraBankData.xlsx file into Power BI) have completed. You should be in the "Report" view, where you see a blank canvas on the left, a "Visualizations" pane on the right (with icons like Pie Chart and Bar Chart), and a "Fields" pane listing your data columns (e.g., CUSTOMER ID, Suspicious Flag).

• Check Your Data:

In the "Fields" pane, ensure you see all columns from your Excel file (CUSTOMER ID, Full Name, DOB, Account Type, Account No., Email Address, Account Balance, Transaction Frequency, Suspicious Flag, Transaction Amount Deviation).

• Set Up Your Canvas: Click on the blank canvas in the Report view to start adding visuals. It can resize or move charts later to make dashboard look neat.

• Tip: Save Power BI file (File > Save As > CanaraBankFraud.pbix) often to avoid losing work.

3.3.2 Visualization 1: Suspicious Transactions (Pie Chart)

Let’s start with a Pie Chart to see how many accounts are suspicious (flagged “Yes” in your Suspicious Flag column) versus non-suspicious (“No).

1. Add the Pie Chart:

   • In the “Visualizations” pane, click the Pie Chart icon (it looks like a circular chart).

   • A blank Pie Chart will appear on canvas.

2. Set Up the Chart:

   • In the “Fields” pane, drag “Suspicious Flag” to the “Legend” box under the Pie Chart’s properties.

   • Drag “CUSTOMER ID” to the “Values” box. In the Values dropdown, select “Count” (this counts how many customers have each flag: Yes or No).

3.Customize It:

   • Click the Pie Chart, then go to the “Format Visual” tab (paint roller icon).

   • Change colors to make “Yes” stand out (e.g., red for Yes, green for No).

   • Add a title: Click “General” in the Format pane, then type “Suspicious vs. Non-Suspicious Accounts” in the Title Text box.

2. What It Shows: This chart shows the percentage of accounts flagged as suspicious. For example, if 50 out of 250 accounts are “Yes,” the pie slice for “Yes” will be 20%.

Example Output: Pie Chart might look like this:

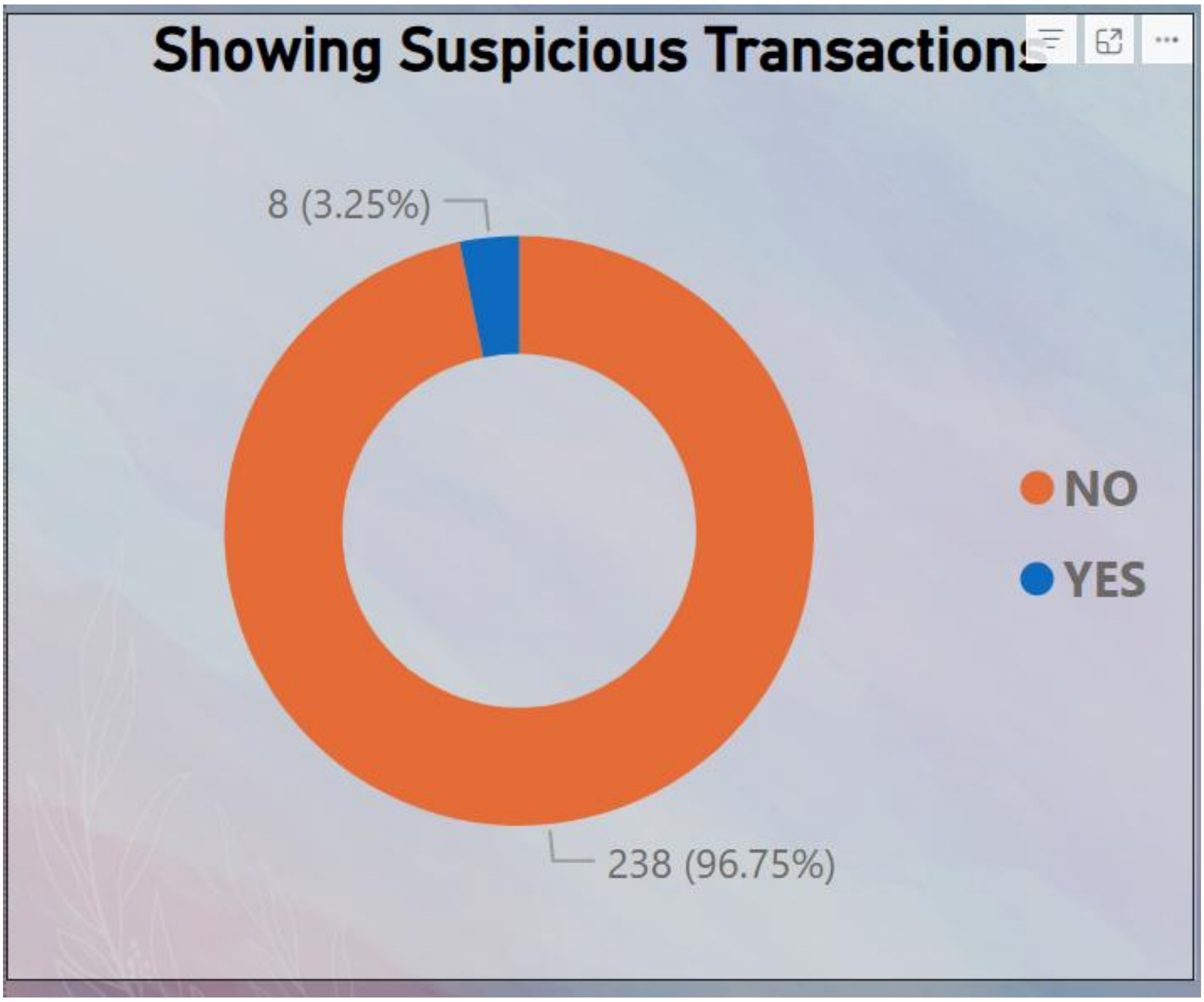


Figure 1: Pie Chart of Suspicious Transactions

3.3.3 Visualization 2: Transaction Frequency vs. Account Balance (Scatter plot)

Next, create a Scatter Plot to spot accounts with high transaction frequency and low balances—prime suspects for fraud. Think of this as a treasure map where each dot is a customer, and the sneaky ones are clustered in a specific corner.

1. **Add the Scatter Plot:**
   - Click the Scatter Plot icon in the "Visualizations" pane (it looks like grid)
   - A blank Scatter Plot appears on your canvas.

2. **Set Up the Chart:**
   - Drag "Transaction Frequency" to the "X-Axis" box.
   - Drag "Account Balance" to the "Y-Axis" box.
   - Drag "Suspicious Flag" to the "Legend" box (this colors dots based on Yes/No).
   - Optionally, drag "Full Name" to the "Tooltips" box to show names when you hover over dots.

3. **Customize It:**
   - In the "Format Visual" tab, adjust dot size for clarity (under "Shapes").
   - Set colours (e.g., red for "Yes," blue for "No").
   - Add a title: "Transaction Frequency vs. Account Balance."
   - Add axis labels: Set X-Axis title to "Transactions per Month" and Y-Axis to "Balance (INR)."

4. 5.What It Shows: Dots on the right (high frequency, >40) and bottom (low balance<50,000) with “yes” flags are fraud suspectors.

Example Output:

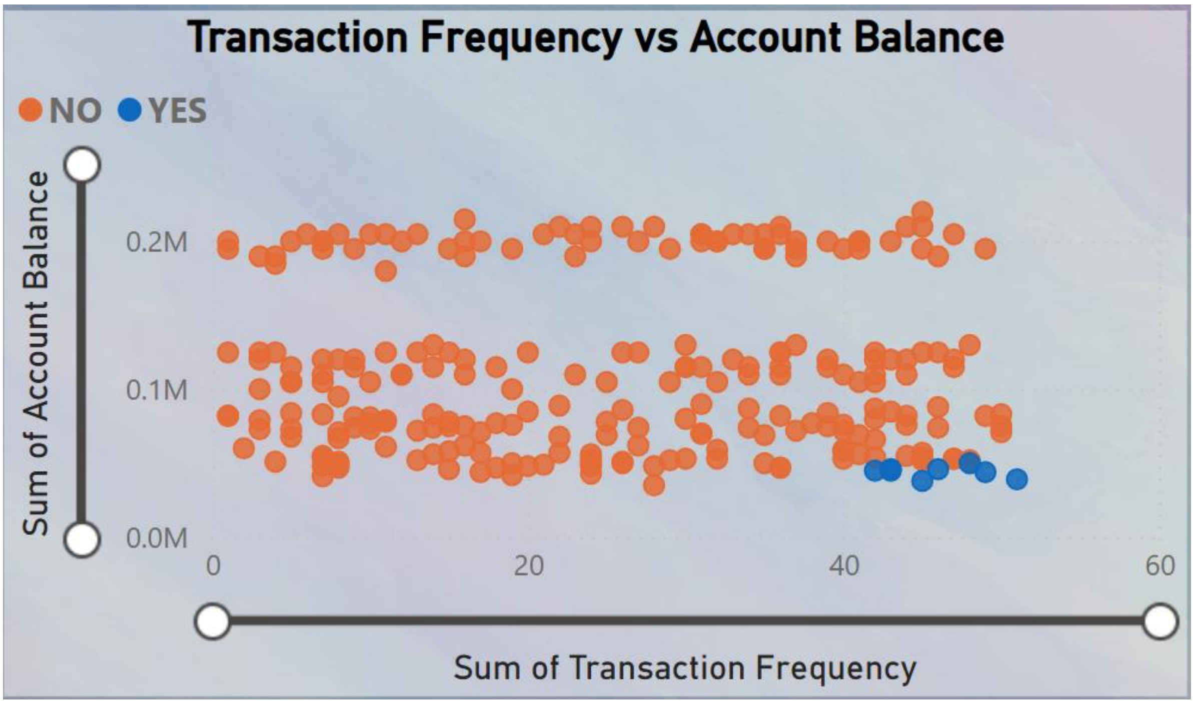


Figure 2: Scatter Plot of Transaction Frequency vs. Account Balance

Troubleshooting:

• Dots Missing: Ensure “Transaction Frequency” and “Account Balance” are numbers, not text, in Power BI. Go to “Transform Data” and set their data types to “Whole Number” and “Currency.”

• Cluttered Plot: If too many dots overlap, use the “Zoom Slider” (in View tab) to explore the chart.

3.3.4 Visualization 3: Account Type-wise Fraud (Bar Chart)

Now, let's see which account types (Savings, Current, Fixed Deposit) have more fraud.

A Bar Chart will stack up the numbers like a scoreboard, showing which account type is the sneakiest.

1. Add the Bar Chart:
    - Click the Bar Chart icon (stacked bars) in the "Visualizations" pane.
    - A blank Bar Chart appears.

2. Set Up the Chart:
    - Drag "Account Type" to the "Axis" box (this creates bars for Savings, Current, Fixed Deposit).
    - Drag "Suspicious Flag" to the "Values" box and set it to "Count" (counts how many accounts of each type are Yes/No).
    - Optionally, drag "Suspicious Flag" to "Legend" to split bars by Yes/No.

3. Customize It:
    - In "Format Visual," set bar colours (e.g., red for Yes, green for No).
    - Add a title: "Fraud by Account Type."
    - Set Axis titles: X-Axis to "Account Type," Y-Axis to "Number of Accounts."

1. What It Shows: Tall bars for "Yes" under Savings or Current suggest those account types need more scrutiny. For example, if Savings has 30 "Yes" accounts, it's a red flag!

Example Output:

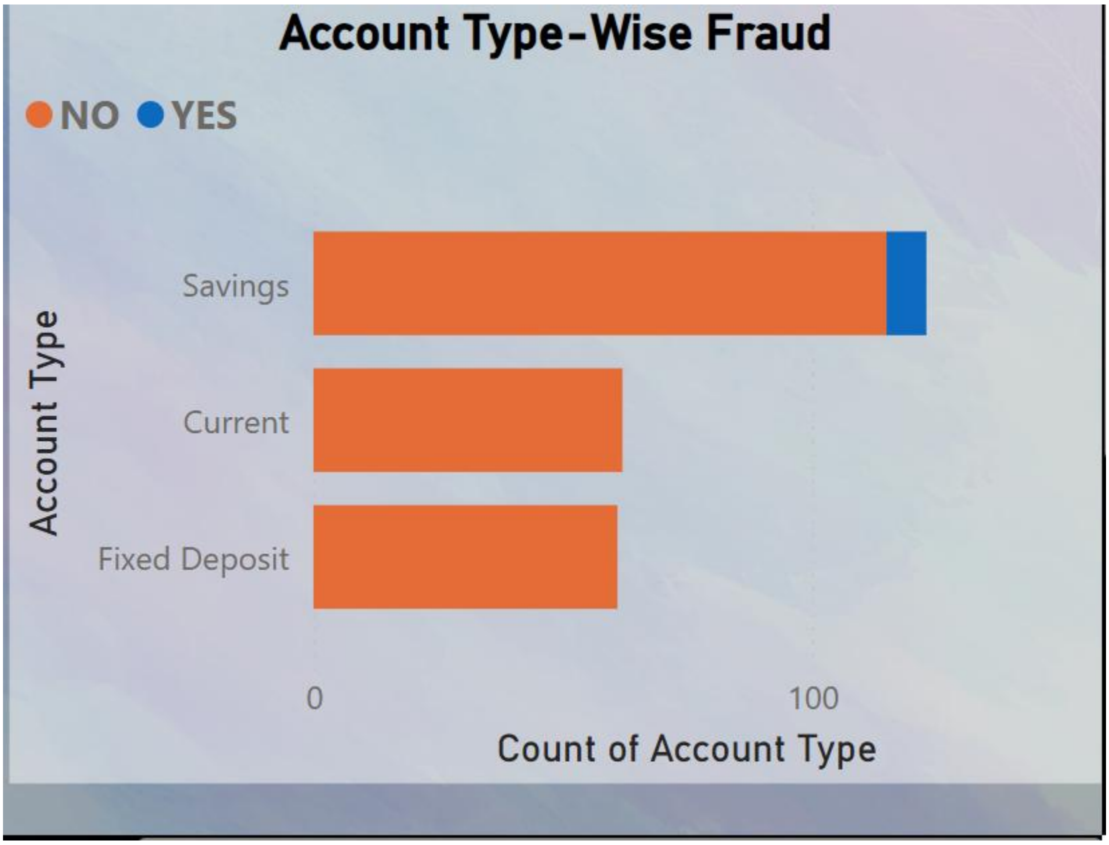


Figure 3: Bar Chart of Fraud by Account Type

3.3.5 Visualization 4: Top Suspicious Customers (Table)

Finally, create a Table to list the top 10 suspicious customers, like a “Most Wanted” list for fraudsters. It helps to zoom in on specific people to investigate.

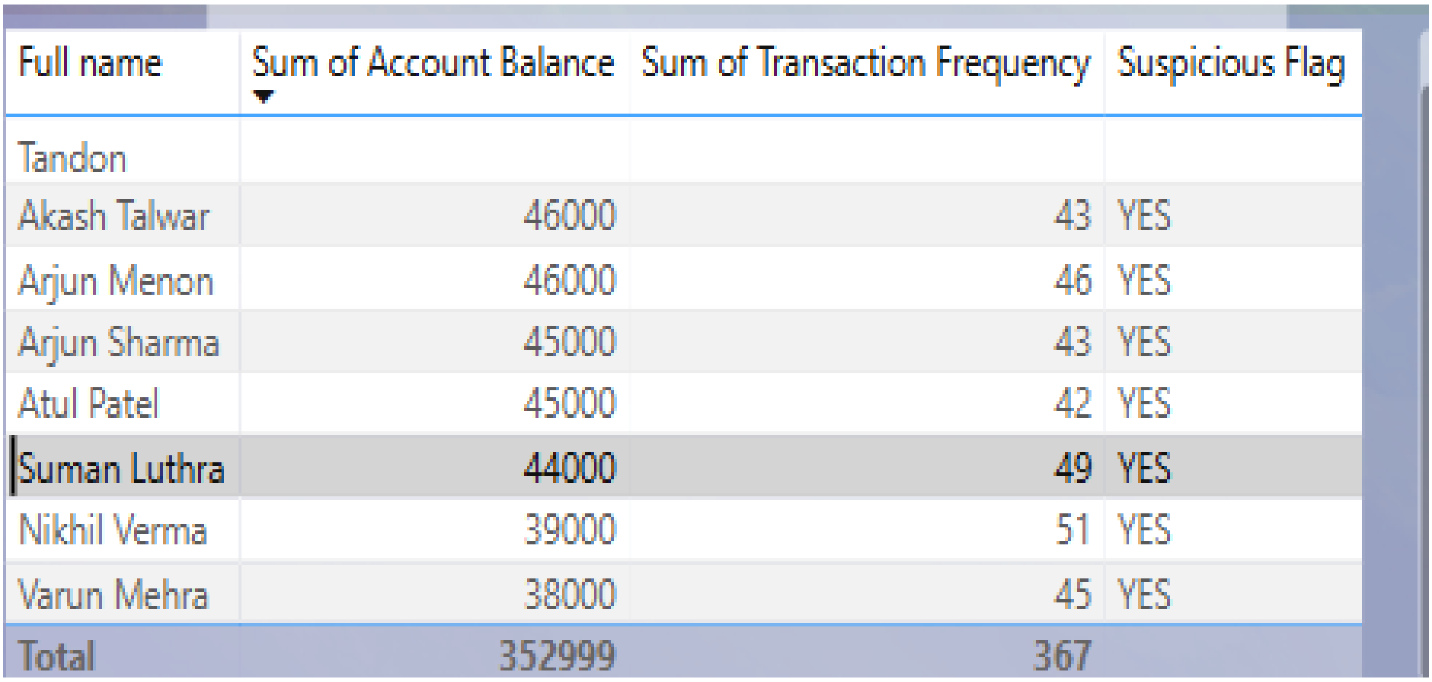
1. Add the Table:
   - Click the Table icon in the “Visualizations” pane (looks like a grid). • A blank Table appears.

2. Set Up the Table:
   - Drag “Full Name,” “Account Balance,” and “Transaction Frequency” to the “Values” box.
   - In the “Filters” pane (right side), add “Suspicious Flag,” set it to “Yes.”

3. Sort the Table:
   - Click the dropdown arrow in the “Transaction Frequency” column header and select “Sort Descending.”
   - To show only the top 10, go to the “Filters” pane, select “Transaction Frequency,” and apply a “Top N” filter (Top 10 by Transaction Frequency).

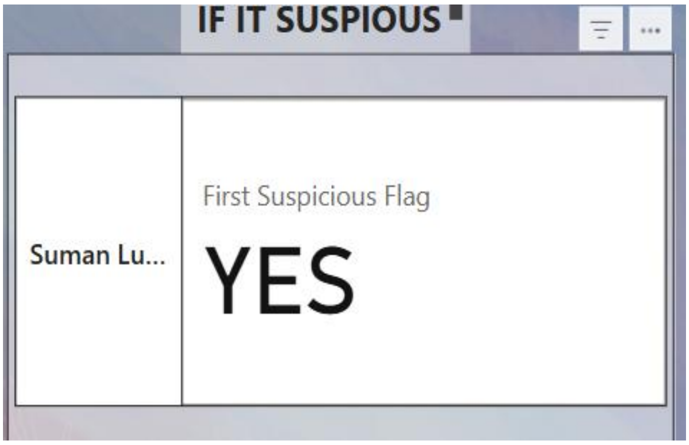
4. Customize It:
   - In “Format Visual,” adjust font size for readability (e.g., 12pt).
   - Add a title: “Top 10 Suspicious Customers.”
   - Format “Account Balance” as currency (₹) in the “Modeling” tab.
5. What It Shows: A list of customers with “Yes” flags, high transaction frequencies, and low balances. For example, “Amit Sharma” with 42 transactions and ₹45,000 balance might top the list

Example Output:



Full name	Sum of Account Balance	Sum of Transaction Frequency	Suspicious Flag
Tandon			
Akash Talwar	46000	43	YES
Arjun Menon	46000	46	YES
Arjun Sharma	45000	43	YES
Atul Patel	45000	42	YES
Suman Luthra	44000	49	YES
Nikhil Verma	39000	51	YES
Varun Mehra	38000	45	YES
Total	352999	367	

Top Suspicious Customers

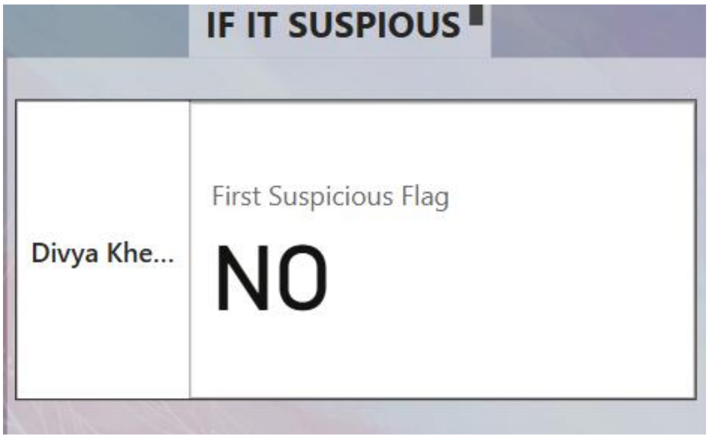


IF IT SUSPIOUS

Suman Lu...

First Suspicious Flag

YES



IF IT SUSPIOUS

Divya Khe...

First Suspicious Flag

NO

Troubleshooting:

- Empty Table: If no rows appear, check the “Suspicious Flag” filter—ensure it’s set to “Yes.”
- Wrong Sorting: If the table isn’t sorted by Transaction Frequency, reapply the “Sort Descending” option.

3.5 Step 5: Insights and Recommendations

Based on the dashboard, the following insights are derived:

• Savings accounts may show higher suspicious transactions, indicating a need for closer monitoring.

• Accounts with high transaction frequency (>45) and low balance (<50,000) are likely fraudulent.

• Fixed Deposit accounts with high transaction frequency are anomalous, as they typically have low activity.

Recommendations for Canara Bank:

• Real-Time Monitoring: Implement a system to monitor transactions in real time, especially for Savings accounts.

• Multi-Factor Authentication (MFA): Mandate MFA for high-risk accounts.

• Customer Education: Educate customers about phishing attacks and fraudulent apps.

- Automated Alerts: Configure Power BI to send alerts for accounts with high transaction frequency.

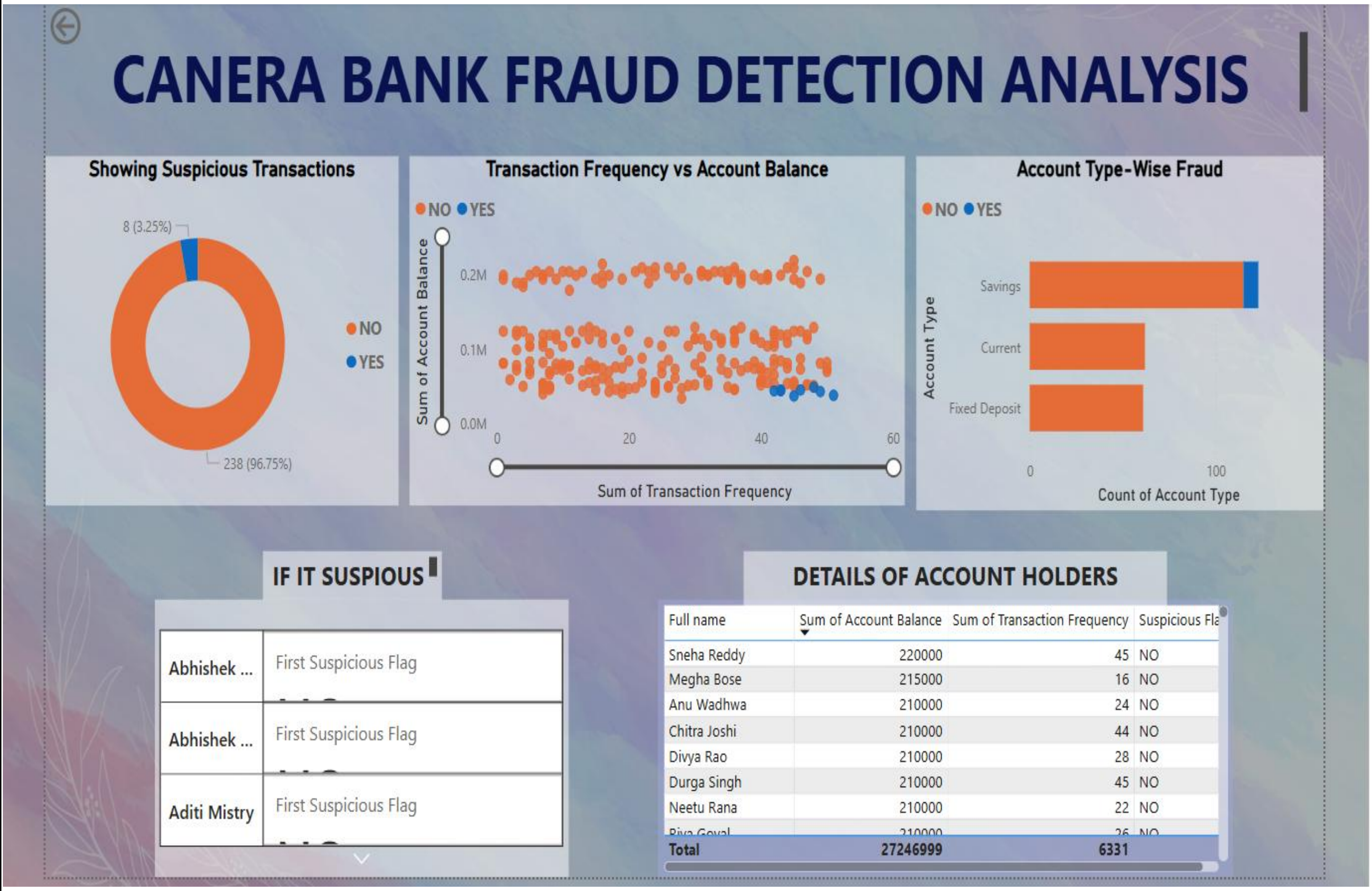
3.6 Step 6: Sharing the Dashboard

1. Click “Publish” in Power BI Desktop to upload the dashboard to Power BI Service.

2. Share the dashboard with project stakeholders via secure links.

   Link: "C:\Users\Lenovo\OneDrive\VI sem Project\Dashboard BI Canera bank FA.pbix"

Final presentation of Canara Bank Fraud Analysis Dashboard



CANERA BANK FRAUD DETECTION ANALYSIS

IF IT SUSPIOUS

Abhishek ...	First Suspicious Flag
Abhishek ...	First Suspicious Flag
Aditi Mistry	First Suspicious Flag

DETAILS OF ACCOUNT HOLDERS

Full name	Sum of Account Balance	Sum of Transaction Frequency	Suspicious Fla
Sneha Reddy	220000	45	NO
Megha Bose	215000	16	NO
Anu Wadhwa	210000	24	NO
Chitra Joshi	210000	44	NO
Divya Rao	210000	28	NO
Durga Singh	210000	45	NO
Neetu Rana	210000	22	NO
Riya Goyal	210000	26	NO
Total	**27246999**	**6331**	

4. Additional Tips

- For real datasets, consider applying Benford's Law to detect anomalies in transaction amounts.
- Use Power BI's interactive features (e.g., slicers, filters) to enhance dashboard usability.
- Explore machine learning models (e.g., anomaly detection) for larger datasets.

5. Sample Data and Visualizations

Below is a sample of the processed dataset (first 5 rows):

ID	Name	DOB	Type	Acc.NO.	Email	Balance	Freq.
1	Amit Sharma	1985-03-15	Savings	123456789	amit@exa.com	45000	42
2	Priya Singh	1990-07-22	Current	987654321	priya@exa.com	75000	25
3	Rajesh Kumar	1978-11-30	Fixed	456789123	rajesh@exa.com	120000	10
4	Sneha Patel	1995-11-30	savings	789123456	sneha@exa.com	30000	48
5	Vikram Rao	1982-09-05	Current	321654987	vikram@exa.com	60000	35

Table 1: Sample Processed Dataset

5.1 Visualization Examples

- Pie Chart: Shows 20% of accounts flagged as suspicious.
- Scatter Plot: Highlights clusters of high-frequency, low-balance accounts.

- Bar Chart: Indicates Savings accounts have the highest fraud incidents.

6. Conclusion

This project demonstrates a robust methodology for fraud analysis using Excel and Power BI. By processing data, creating insightful visualizations, the analysis identifies suspicious patterns and provides actionable recommendations. The approach is scalable and can be adapted for real-time fraud detection with actual bank data.

- Summary:
    - Step 1: Organized Data in Excel
    - Step 2: Imported Data into Power BI
    - Step 3: Created Cool Charts:
    - Step 4: Set Smart Rules
    - Step5: Found Insights and Suggestions
    - Step 6: Shared Your Work

- Learning Outcomes
    - Data Cleaning
    - Data Visualization
    - Analytical Thinking
    - Presentation Skills

7. Appendices

Excel Formulas -

- Transaction Frequency: =RANDBETWEEN (1,50)

- Suspicious Flag: =IF (AND (G5<50000, H5>40),”Yes” , ”No”)
- Transaction Amount Deviation: = G2*0.05 + RANDBETWEEN (-1000, 1000)

8. Suggestion

1. Keeping an Eye on Risky Accounts
    a. Set Up Real-Time Alerts
    b. Prioritize Savings Accounts
2. Locking Down Accounts with Extra Security
3. Teaching Customers to Outsmart Scams

9. References

- Power BI Documentation: https://docs.microsoft.com/en-us/power-bi/
- Excel Data Analysis Techniques: General knowledge resources.
- Fraud Detection Best Practices: Industry standards for banking.

THANKYOU