**Anomaly Detection in Credit Card Transactions using Power BI**

**About:-**

Anomaly detection in credit card transactions is a critical process aimed at identifying uncommon or potentially fraudulent activities within credit card transactions. This procedure employs a combination of statistical analysis, machine learning algorithms, and data visualisation tools, such as Power BI, to uncover irregular patterns and deviations from typical transaction behaviour. The ultimate goal is to swiftly detect and flag transactions that may be fraudulent in real-time, safeguarding the financial integrity of credit card holders and financial institutions.

**Project Overview:**

The primary objective of this project is to design and implement a comprehensive Power BI dashboard tailored for anomaly detection in credit card transactions. Anomaly detection plays a pivotal role in safeguarding the integrity of credit card transactions by promptly identifying and mitigating fraudulent activities. By harnessing the robust data visualisation and analytical features of Power BI, we aim to develop an interactive and informative dashboard. This dashboard will offer valuable insights into transaction trends, empowering users to spot potential anomalies efficiently, thus enhancing the security of credit card transactions.

**Project Steps:**

**—----------------------------------------**

* **Dataset Info:**
* ***step*** - maps a unit of time in the real world. In this case 1 step is 1 hour of time. Total steps 744 (30 days simulation).
* ***type*** - CASH-IN, CASH-OUT, DEBIT, PAYMENT and TRANSFER.
* ***amount*** - amount of the transaction in local currency.
* ***nameOrig*** - customer who started the transaction
* ***oldbalanceOrg*** - initial balance before the transaction
* ***newbalanceOrig*** - new balance after the transaction
* ***nameDest*** - customer who is the recipient of the transaction
* ***oldbalanceDest*** - initial balance recipient before the transaction. Note that there is no information for customers that start with M (Merchants).
* ***newbalanceDest*** - new balance recipient after the transaction. Note that there is no information for customers that start with M (Merchants).
* ***isFraud*** - This is the transactions made by the fraudulent agents inside the simulation. In this specific dataset the fraudulent behaviour of the agents aims to profit by taking control of customers accounts and try to empty the funds by transferring to another account and then cashing out of the system.

In order to commence our project, it is essential to initiate by importing the provided dataset and then meticulously process it by addressing missing values, ensuring data integrity, and performing necessary transformations to prepare it for analysis accordingly.

* **Power BI Dashboard Creation:**
* Firstly, we need to Launch Power BI and connect it to the preprocessed credit card transaction dataset.
* Then, I have designed an intuitive and visually appealing dashboard layout with appropriate charts, tables, and filters.
* And then created the visualisations that provide an overview of transaction statistics, such as total transactions, average transaction amount, and transaction frequency as well.
* **Data Preprocessing:**
* At this stage we will perform the data cleaning tasks, such as handling missing values and duplicates if needed.
* Then we need to transform the data into a format suitable for Power BI, ensuring proper data types.
* **DAX Function:**

Average Transaction Amount :

* DAX Function: Average Transaction Amount = AVERAGE('Transactions'[Amount])
* We use this function to calculate and compare the average transaction amount for normal and fraudulent transactions, providing insight into potential discrepancies.

Count of Transactions:

* DAX Function: Total Transactions = COUNTROWS('Transactions')
* DAX Function: Total Fraudulent Transactions = COUNTROWS(FILTER('Transactions', 'Transactions'[IsFraudulent] = TRUE))
* These functions help determine the total number of transactions and the count of fraudulent transactions in the dataset.

Highest Fraud Transaction Amount:

* DAX Function: Highest Fraud Amount = MAXX(FILTER('Transactions', 'Transactions'[IsFraudulent] = TRUE), 'Transactions'[Amount])
* This function identifies the highest transaction amount among fraudulent transactions, assisting in fraud detection and analysis.

Maximum Transaction Amount Comparison:

* We perform a comparison between the maximum transaction amount for normal and fraudulent transactions to assess significant differences using DAX expressions like MAX and FILTER.

Percentage of Fraudulent Transactions:

* DAX Function: Percentage of Fraudulent Transactions = [Total Fraudulent Transactions] / [Total Transactions]
* This function calculates the percentage of fraudulent transactions, a crucial metric for monitoring transaction security.

Distribution of Transaction Amounts:

* We create a clustered column chart using DAX to visualize the distribution of transaction amounts, providing a clear view of transaction patterns and potential anomalies.
* **Chart types:**

1.A line chart is best for "Average Transaction and Average Fraudulent Transaction By Types of Transaction" because it:

* Tracks trends effectively.
* Allows easy comparisons.
* Emphasizes smooth data changes.
* Clarifies relationships.

2..Clustered column charts are ideal for visualizing the" Highest fraudulent and Highest normal transactions because they:

* Allow clear side-by-side comparison.
* Highlight outliers effectively.
* Categorically represent data.
* Convey information visually, making it easy to grasp the problem's significance.

3.Clustered column charts are best for visualizing "Total transactions by types Of Transaction" for four main reasons:

* Comparison: They allow easy comparison of transaction types.
* Clarity: Columns are grouped, ensuring neat organization.
* Trend Identification: Trends over time or across categories are visible.
* Decision Support: They aid decision-making by offering a clear summary.

4.Using a scatter chart to visualize "Payer Old Balance" vs. "Transaction Amount" is effective because it:

* Identifies Outliers: Helps spot unusual transactions.
* Reveals Patterns: Shows typical transaction behavior.
* Assesses Correlation: Highlights relationships between variables.
* Displays Data Density: Indicates where transactions cluster, aiding decision-making.

5.Line Chart for "Total Transactions by Hour":

* Trend Tracking: Line charts show how transaction counts change throughout the day, making it easy to identify peak hours and trends.
* Continuous Data: Ideal for displaying continuous data like hourly transaction counts, providing a smooth representation.
* Comparative Analysis: Allows straightforward comparison of transaction activity between different hours.
* Anomaly Detection: Effective at spotting anomalies or irregular patterns, aiding in problem identification.

6.Using a table for the "Top 10 Merchants Transaction" data is best because:

* Offers immediate clarity.
* Facilitates efficient comparisons.
* Reveals patterns and trends.
* Enhances communication of insights.

**Power BI Dashboard Overview:**

* Our Power BI dashboard is designed to empower financial institutions and businesses with actionable insights to combat credit card fraud. It offers a user-friendly interface with the following key elements.
* Prominent display of key metrics, including average transaction amounts, total transactions, total fraudulent transactions, highest fraud amount, and the percentage of fraudulent transactions.
* Transaction Distribution Chart: A clustered column chart showcases the distribution of transaction amounts for quick trend and anomaly identification.
* Comparison Insights: Visual comparison of maximum transaction amounts for normal and fraudulent transactions highlights potential fraud indicators.
* Drill-Down Functionality: Users can explore specific time periods, card types, or other dimensions for detailed transaction insights.
* Real-Time Monitoring: Support for real-time data updates ensures users can track and respond to anomalies as they occur.

By methodically following the steps outlined above, we've achieved the creation of a robust Power BI project centered around anomaly detection in credit card transactions. This project is poised to empower users with powerful tools for the swift identification and response to potential fraud.

Our project aligns seamlessly with the highest standards of project submission, ensuring that stakeholders have access to a comprehensive system that enhances their ability to safeguard financial transactions. With its user-friendly interface, real-time data updates, customizable filters, and actionable insights, this Power BI project equips organizations to proactively combat credit card fraud, promoting financial security and trust within the industry.