**Name:** Harvy Doshi

**Roll Number:** 22BCE084

**Batch:** B1

**Course Code & Name:** 3CS103ME24 Data Analysis and Visualization

**Practical:** 1

**Aim:** Study and explore different domains such as Retail, Healthcare, Education, E- commerce, Media & Entertainment, Finance, Travel Industry, Telecom, and Automobile etc., and select a domain of choice to study. Perform the following tasks:

* Identify and discuss the various applications of the selected domain and select one application for study.
* Find a suitable data set related to the application selected and discuss the following for the selected application:
* importance,
* issues and challenges
* stakeholders
* usage of the application for each stakeholder

Domain: Credit Card Fraud Detection in E-commerce

**1. Identify and Discuss the Various Applications:**

In the context of e-commerce, credit card fraud detection entails spotting unlawful or questionable activity on websites. This domain's primary uses are as follows:   
  
- Real-time Transaction Monitoring: Preventing losses by seeing fraudulent transactions as soon as they happen.   
- User Behavior Analysis: Examining usage habits to find deviations that might point to fraud.   
- Charge-back Prevention: Preventing charge-backs, which can be expensive for retailers, by identifying fraudulent activity.   
- Risk Scoring: Based on a number of factors, including transaction size, location, and past purchases, risk scores are assigned to individual transactions.

- Anomaly Detection: This technique looks for departures from typical purchasing behavior using machine learning models.   
  
Real-time Transaction Monitoring is the study's chosen application.   
  
**2. Discussion and Dataset Selection:**   
  
We can use a dataset similar to the "Credit Card Fraud Detection" dataset on Kaggle for this investigation.

Link: <https://www.kaggle.com/datasets/kalyankaparaju01/credit-card-fraud-detection-dataset?resource=download>

Attributes: Index, trans\_date, trans\_time, cc\_num, merchant, category, amt, first, last, gender, street, city, state, zip, lat,long, city\_pop, job, dob, trans\_num, unix\_time, merch\_lat, merch\_long, is\_fraud

**3. Transaction Monitoring in Real-Time Is Important:**  
- Fraud Prevention: By instantly identifying and rejecting questionable transactions, real-time monitoring helps businesses and consumers avoid financial losses.   
- Customer Trust: Businesses may preserve and grow their customer base's loyalty by shielding users from dishonest practices.   
- Regulatory Compliance: A lot of financial regulations mandate that companies put fraud detection and prevention procedures in place. Monitoring in real time makes it easier to comply with these demands.   
- Cost Reduction: Businesses can cut expenses related to chargebacks, lawsuits, and compensations by eliminating fraud.

**4. Problems and Difficulties:**   
  
- False Positives: When normal transactions are mistakenly reported as fraudulent, leading to customer annoyance, this is one of the largest problems in fraud detection.   
- Changing Fraud Techniques: Since fraudsters are always changing their strategies, it is difficult to maintain detection systems current.   
- Data Privacy: It's critical to handle sensitive consumer data while maintaining privacy and adhering to data protection regulations.   
- Scalability: The system must be able to grow effectively without sacrificing accuracy as the number of transactions rises.   
- Latency: To prevent delays in the user experience, real-time monitoring necessitates a minimum amount of latency in transaction processing.

**5. Entities Affected:**   
  
  
- Customers: The main parties affected by fraud directly are the customers. To safeguard their monetary holdings, they depend on these mechanisms.   
- Merchants: To safeguard their profits, lower chargebacks, and uphold client confidence, they require fraud detection systems.   
- Banks and other financial institutions: They handle payment processing and verify the validity of transactions.   
-Regulatory Bodies: Establishing bodies that establish policies and rules pertaining to the identification and avoidance of fraud.   
- Technology Providers: Businesses that create the algorithms and software used by banks and retailers to detect fraud.

**6. Application Use for Every Stakeholder:**   
  
- Clients: Take advantage of safe transactions and a lower chance of suffering financial loss as a result of fraud.   
- Merchants: Lower chargeback rates and safeguard money by using real-time monitoring to stop fraudulent transactions.   
- Banks and other financial institutions should integrate fraud detection into their transaction processing procedures in order to abide by rules and protect themselves from financial hazards.   
- Regulatory Bodies: Keep an eye on fraud detection systems' efficacy to make sure they safeguard customers and adhere to regulatory requirements.   
- Technology Providers: In order to stay ahead of emerging risks and provide strong security for all parties concerned, constantly update and improve fraud detection algorithms.