CREDIT CARD FRAUD DETECTION

PHASE 3 PROJECT SUBMISSION

TOPIC: START BUILDING THE CREDIT CARD DETECTION PROJECT BY LOADING AND PRE-PROCESSING THE DATASET

Introduction:

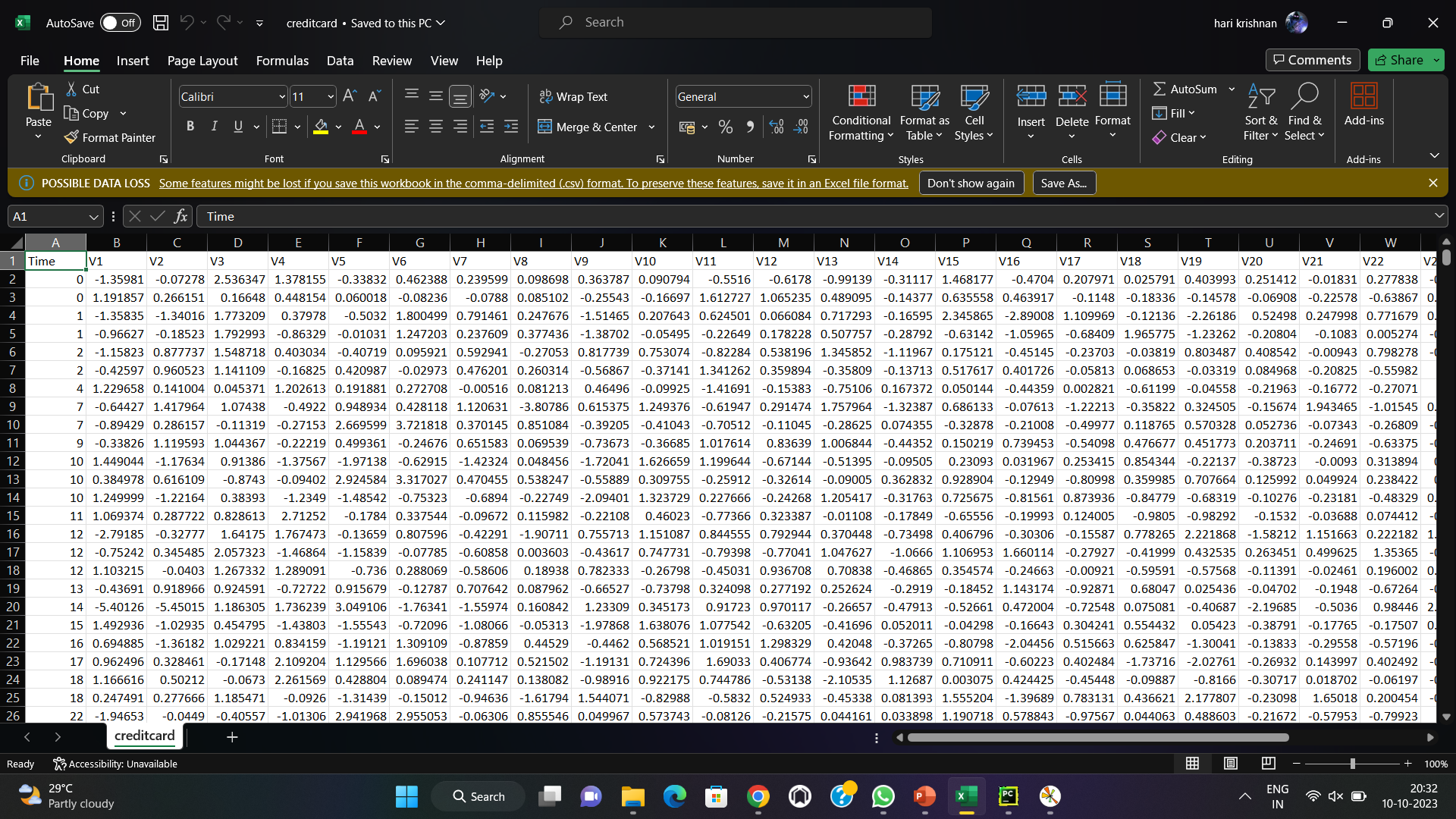
* **Data Collection**: Financial institutions collect a vast amount of data related to card transactions, including transaction amount, location, date and time, merchant information, and more. This data forms the basis for fraud detection.
* **Machine Learning and Artificial Intelligence**: Machine learning algorithms and AI models play a pivotal role in analyzing the data. They are trained to identify patterns, anomalies, and trends associated with legitimate and fraudulent transactions. Common algorithms include decision trees, neural networks, logistic regression, and random forests.
* **Rules-Based Systems**: In addition to machine learning, rules-based systems are used to set predefined rules that can trigger alerts or actions when certain conditions are met. These rules may include transaction amount limits, transaction frequency thresholds, and location-based checks.
* **Behavioral Analysis**: By monitoring a cardholder's behavior over time, financial institutions can establish a baseline of normal activity. Deviations from this baseline, such as an unusual transaction in a different location or an unusually large purchase, can raise red flags.
* **Real-time Monitoring**: Many systems operate in real-time, continuously assessing incoming transactions as they occur. This allows for immediate responses to potential fraud, such as flagging a transaction for manual review or blocking a card.
* **Historical Data Analysis**: Historical transaction data is invaluable for identifying recurring fraud patterns. By analyzing past incidents, financial institutions can refine their fraud detection models and rules.
* **Machine Learning Model Training**: Regular updates and retraining of machine learning models are essential to adapt to evolving fraud tactics. New data helps models become more accurate in recognizing fraudulent behavior.
* **Customer Verification**: Multi-factor authentication, including something the cardholder knows (e.g., PIN), something the cardholder has (e.g., the card itself), and something the cardholder is (e.g., biometrics), can provide an extra layer of security.
* **Collaboration**: Financial institutions often collaborate with industry organizations and share fraud intelligence to stay ahead of emerging threats and trends.
* **Customer Alerts**: Providing cardholders with alerts for suspicious activity via text messages, emails, or mobile apps allows them to quickly report unauthorized transactions.

Dataset:

The dataset for the given credit card fraud detection project can be downloaded from the link given below.

<https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud/code>

The given dataset is picturized as below:



Loading and pre-processing of dataset:

Loading and pre-processing the dataset is an important first step in building up any machine learning model. However ,it is especially important for credit card fraud detection dataset are complex and noisy.

1.LOADING THE DATASET:

* To load a dataset for credit card fraud detection, you can follow these steps:
* as Pandas, **Choose a Dataset**: There are several publicly available datasets for credit card fraud detection, which you can use for research or model development. One of the most commonly used datasets is the Credit Card Fraud Detection dataset available on Kaggle. You can download this dataset or use other reputable sources like the UCI Machine Learning Repository.
* **Import Python Libraries**: You'll typically use Python for data analysis and machine learning. Import libraries such NumPy, and Scikit-Learn to manipulate and work with the dataset.

PROGRAM:

Since we are given two datasets, we are going to load both of these datasets separately.

import pandas as pd

import numpy as np

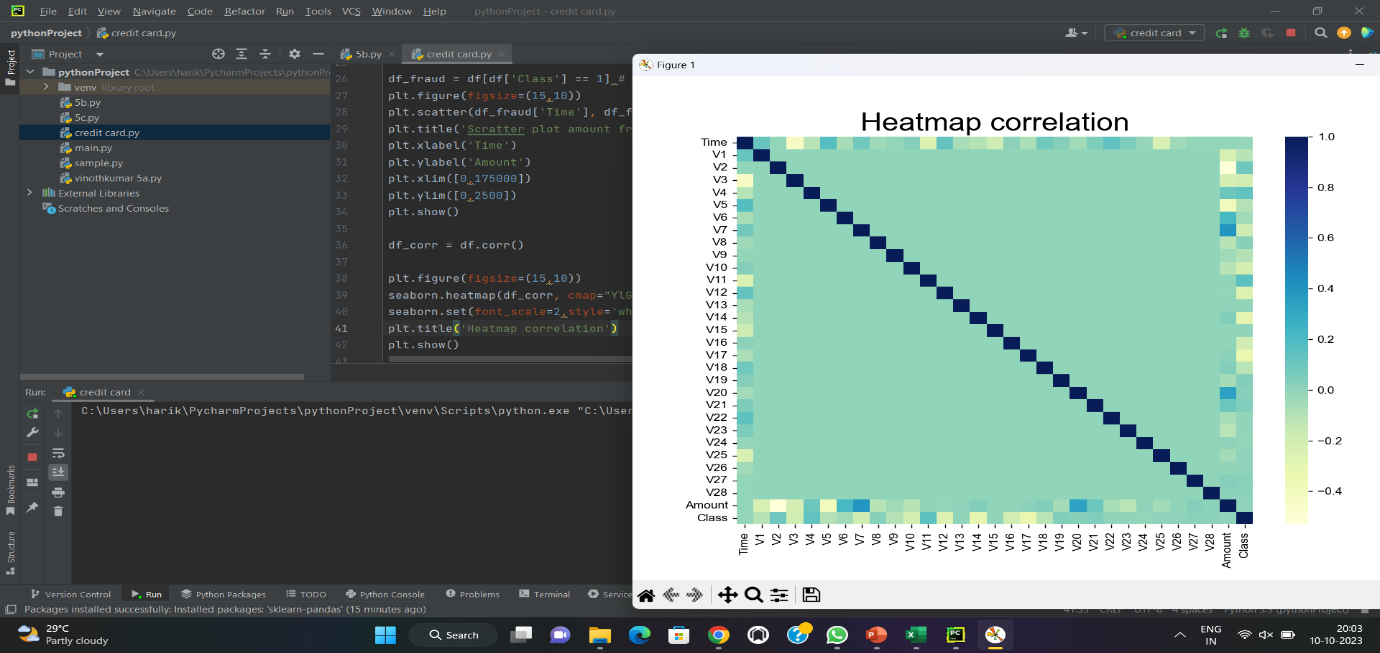
data = pd.read\_csv('filename.csv')

from sklearn.model\_selection import train\_test\_split

X = data.drop('Class', axis=1)

y = data['Class']

X\_train, X\_test, y\_train, y\_test = train\_test\_split(X, y, test\_ size=0.3, random\_state=42)

Output:

2.PRE-PROCESSING THE DATASET:

Preprocessing the data in a credit card fraud detection dataset is a crucial step to ensure that the data is ready for machine learning. The goal of preprocessing is to clean and prepare the data, making it suitable for training a model that can effectively detect fraudulent transactions. Here are the common preprocessing steps for credit card fraud detection:

import pandas as pd

import numpy as np

*# Scikit-learn library: For SVM*

from sklearn import preprocessing

from sklearn.metrics import confusion\_matrix

from sklearn import svm

df\_fraud = df[df['Class'] == 1] *# Recovery of fraud data*

plt.figure(figsize=(15,10))

plt.scatter(df\_fraud['Time'], df\_fraud['Amount']) *# Display fraud amounts according to their time*

plt.title('Scratter plot amount fraud')

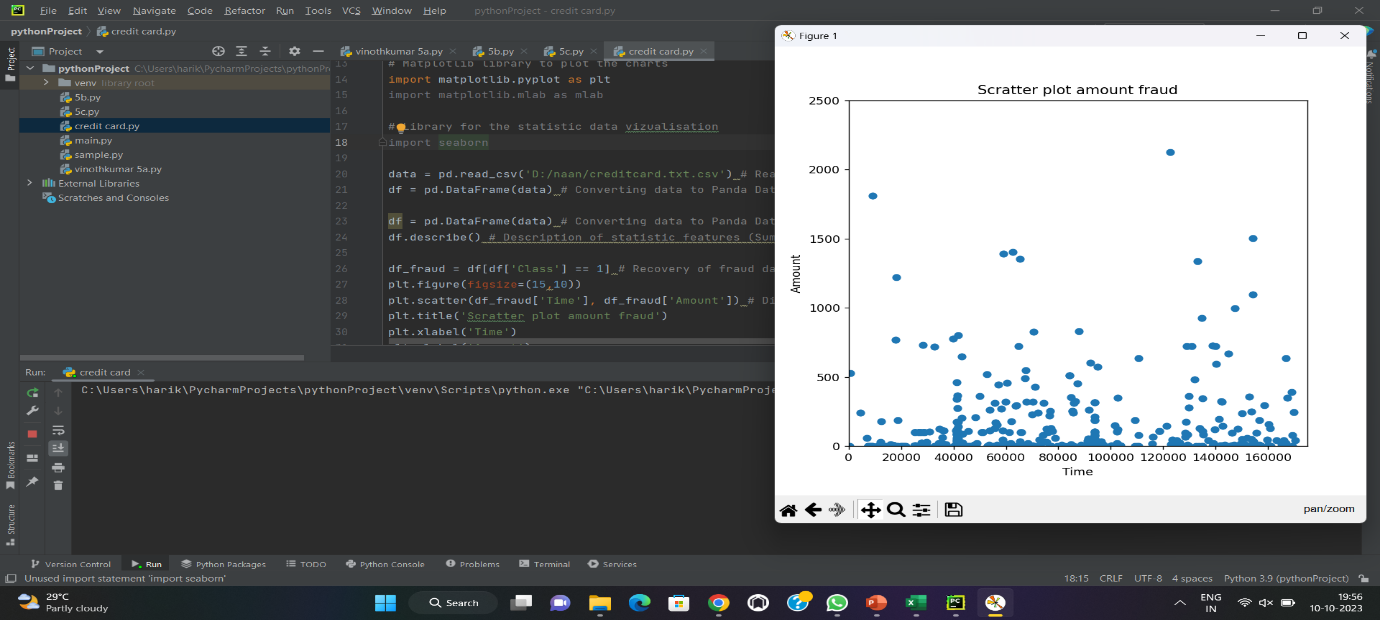
plt.xlabel('Time')

plt.ylabel('Amount')

plt.xlim([0,175000])

plt.ylim([0,2500])

plt.show()

OUTPUT: 

CONCLUSION:

In conclusion, credit card fraud detection is a critical aspect of financial security in today's digital age. Fraudulent activities can result in significant financial losses, damage to a financial institution's reputation, and harm to cardholders. To combat this threat effectively, credit card fraud detection systems rely on data analysis, machine learning, and various preprocessing steps to prepare the data for modeling. Here are the key takeaways:

* \*\*Importance of Credit Card Fraud Detection\*\*: Credit card fraud poses a substantial risk to financial institutions and cardholders, necessitating advanced fraud detection methods.
* \*\*Data Preprocessing\*\*: Preprocessing the dataset is a vital step, involving data cleaning, handling class imbalance, scaling, feature engineering, encoding, dimensionality reduction, and splitting the data into training and testing sets.