Credit Card Fraud Detection

Team members:

Abhijith SS - 961721104001

Adarsh LS - 961721104003

Anandhu S - 961721104302

Ashkar Muhammad AM - 961721104305

Akhil SS - 961721104301

Phase 3 Submission Document

Project: Credit Card Fraud Detection

Introduction:

* **Protecting Consumers: Prevents unauthorized transactions andidentity theft.**
* **Protecting Businesses: Safeguards against revenue loss and reputational damage.**
* **Reducing Financial Losses: Minimizes financial impact onndividuals and organizations.**
* **Maintaining Trust in the Financial System: Ensures confidencein payment networks.**
* **Future Developments :**we need credit card fraud detection techniques**to protect the cardholders from false activity.** India is on its way to becoming a developed country. To achieve this, the Government of India (GoI) has launched several initiatives and one of these is Digital India Campaign.

Content for Project Phase 3 :

For analyzing data, we need some libraries. In this section, we are importing all the required libraries like pandas, NumPy, matplotlib, plotly, seaborn, and word cloud that are required for data analysis. Check the below code to import all the required libraries.

Data Source

A good data source for credit card fraud detection should be Accurate, Complete, Covering the geographic area of interest, Accessible.

# Data Collection and Preprocessing:

* Data collection : With Credit Card Fraud Detection, this project demonstrates the modelling of a data collection using **machine learning**. Modeling prior credit card transactions with data from those that turned out to be fraudulent is part of the Credit Card Fraud Detection Problem. The model is then used to determine whether or not a new transaction is fraudulent.

# Data preprocessing: Analyzing the effect of data preprocessing techniques using machine learning algorithms on the diagnosis of fraud detection

# Exploratory Data Analysis ( EDA ):

# This case study is focused to give you an idea of applying Exploratory Data Analysis (EDA) in a real business scenario. In this case study, apart from applying the various Exploratory Data Analysis (EDA) techniques, you will also develop a basic understanding of risk analytics and understand how data can be utilized in order to minimise the risk of losing money while lending to customers.

# Feature Engineering:

**Feature engineering** is a crucial step in credit card fraud detection. It involves selecting and transforming the most relevant features from the dataset to improve the performance of machine learning models. [In credit card fraud detection, feature engineering can help identify patterns and anomalies in transaction data that are indicative of fraudulent activity](https://medium.com/dataman-in-ai/how-to-create-good-features-in-fraud-detection-de6562f249ef).

Advanced Regression Techniques:

# There are several machine learning techniques that can be used for credit card fraud detection. One such technique is **logistic regression**. [In a study, researchers investigated the use of logistic regression to detect fraudulent credit card transactions in an imbalanced dataset where only a small fraction of transactions are fraudulent](https://ieeexplore.ieee.org/document/10112302/).Another technique is **genetic algorithm (GA)** based feature selection. A recent paper proposed a machine learning based credit card fraud detection engine using the GA algorithm for feature selection. [After the optimized features are chosen, the proposed detection engine uses the following ML classifiers: Decision Tree (DT), Random Forest (RF), Logistic Regression (LR), Artificial Neural Network (ANN), and Naive Bayes (NB) 2](https://journalofbigdata.springeropen.com/articles/10.1186/s40537-022-00573-8). [The paper also demonstrated that their proposed approach outperforms existing systems](https://journalofbigdata.springeropen.com/articles/10.1186/s40537-022-00573-8).

# Model Interpretability:

Credit card fraud is a growing problem in the financial industry, with the potential to cause significant

financial losses to both customers and financial institutions. As a result, there has been a significant

amount of research in recent years on developing effective fraud detection systems. These systems rely on

a combination of statistical techniques, machine learning algorithms, and deep learning models to identify

fraudulent transactions.One of the most commonly used approaches for credit card fraud detection is

rule-based systems. These systems use predefined rules to identify transactions that are deemed suspicious.

However, rule-based systems have limitations, as they are only as good as the rules that have been

predefined, and they may not be able to detect new types of fraud. To overcome these limitations, machine

learning algorithms and statistical techniques have been applied to credit card fraud detection. These

techniques are based on analysing transaction-related data, such as the transaction amount, location, and

time, as well as other relevant factors, such as the customer’s transaction history and account details. In

recent years, deep learning models, such as convolutional neural networks (CNNs) and recurrent neural

networks (RNNs), have also been applied to credit card fraud detection. These models have shown

promising results in identifying fraudulent transactions by learning patterns in the data and improving the

accuracy of fraud detection. Overall, credit card fraud detection is a critical area of research in the financial

industry, with significant potential for improving fraud detection rates and reducing financial losse

Credit card fraud is a growing problem in the financial industry, with the potential to cause significant

financial losses to both customers and financial institutions. As a result, there has been a significant

amount of research in recent years on developing effective fraud detection systems. These systems rely on

a combination of statistical techniques, machine learning algorithms, and deep learning models to identify

fraudulent transactions.One of the most commonly used approaches for credit card fraud detection is

rule-based systems. These systems use predefined rules to identify transactions that are deemed suspicious.

However, rule-based systems have limitations, as they are only as good as the rules that have been

predefined, and they may not be able to detect new types of fraud. To overcome these limitations, machine

learning algorithms and statistical techniques have been applied to credit card fraud detection. These

techniques are based on analysing transaction-related data, such as the transaction amount, location, and

time, as well as other relevant factors, such as the customer’s transaction history and account details. In

recent years, deep learning models, such as convolutional neural networks (CNNs) and recurrent neural

networks (RNNs), have also been applied to credit card fraud detection. These models have shown

promising results in identifying fraudulent transactions by learning patterns in the data and improving the

accuracy of fraud detection. Overall, credit card fraud detection is a critical area of research in the financial

industry, with significant potential for improving fraud detection rates and reducing financial losse

Credit Card Fraud can be defined as a case where a person uses someone else’s credit card for personal reasons while the owner and the card-issuing authorities are unaware of the fact that the card is being used. Due to the rise and acceleration of E-Commerce, there has been a tremendous use of credit cards for online shopping which led to High amount of frauds related to credit cards. In the era of digitalization, the need to identify credit card frauds is necessary. Fraud detection involves monitoring and analyzing the behaviour of various users to estimate detect or avoid undesirable behaviour. To identify credit card fraud detection effectively, we need to understand the various technologies, algorithms and types involved in detecting credit card frauds. The algorithm can differentiate transactions which are fraudulent or not. Find fraud, they need to passed dataset and knowledge of the fraudulent transaction. They analyze the dataset and classify all transactions. Fraud detection involves monitoring the activities of populations of users to estimate, perceive or avoid objectionable behaviour, which consist of fraud, intrusion, and defaulting. Machine learning algorithms are employed to analyses all the authorized transactions and report the suspicious ones. These reports are investigated by professionals who contact the cardholders to confirm if the transaction was genuine or fraudulent. The investigators provide feedback to the automated system which is used to train and update the algorithm to eventually improve the fraud-detection performance over time.

Feature Importance Analysis:

Understanding which features or variables have the most significant impact on the model's predictions is often essential. Techniques like feature importance scores (e.g., Gini importance for decision trees or SHAP values) can help highlight the most influential features.

Partial Dependency Plots (PDP):

PDPs illustrate how a model's output changes with variations in a specific feature while holding other features constant. This allows users to see the relationship between individual features and the model's predictions.

LIME (Local Interpretable Model-Agnostic Explanations):

LIME is a technique that provides local interpretability for black-box models. It generates locally faithful explanations by training a simple, interpretable model on a subset of data around a specific prediction. This helps understand the model's behavior in the vicinity of a particular data point.

SHAP (SHapley Additive exPlanations):

SHAP values provide a unified measure of feature importance. They can explain how each feature contributes to a specific prediction and can also give a global view of feature importance.

Decision Trees and Rule-Based Models:

Decision trees are inherently interpretable. By visualizing the tree structure, users can see how decisions are made at each node based on specific features. Rule-based models, like decision sets, provide a set of easy-to-understand rules for predictions.

Counterfactual Explanations:

Counterfactual explanations offer insights into how changing specific feature values would have led to different model predictions. They help users understand what they can do differently to achieve a desired outcome.

Model-Agnostic Methods:

Techniques like SHAP, LIME, and anchor explanations work with any type of model. They provide a way to explain complex models, even if you don't know the internal workings of the model.

Visual Explanations:

Visualization tools can be used to present model interpretations in a more understandable and user-friendly manner. For instance, you can use heatmap visualizations to show how feature values influence predictions.

Global vs. Local Interpretability:

Models can provide global explanations that apply to the entire model or local explanations that focus on a specific prediction. Both types are important depending on the context and audience.

Regulatory Compliance:

In regulated industries like finance, ensuring that a model's behavior aligns with legal and compliance requirements is critical. Transparent and interpretable models are often favored in such scenarios.

Stakeholder Collaboration:

Collaboration between data scientists, domain experts, and business stakeholders can help bridge the gap between technical understanding and practical interpretation.

Documented Model Behavior:

Clearly documenting a model's behavior, including its input features and how it makes predictions, can aid in understanding and interpretation.

Model interpretability is vital not only for understanding model decisions but also for building trust and ensuring that models behave as expected, especially in applications where errors or misclassifications can have significant consequences, such as credit card fraud detection.

# Deployment and Prediction:

Deploy the chosen regression model to credit card fraud detection

Develop a user-friendly interface for users to input property features.

Program:

### Credit Card Fraud Detection

$ pip install sklearn==0.24.2 imbalanced-learn numpy pandas matplotlib seaborn

Let's import the necessary libraries:

import numpy as np

import pandas as pd

import matplotlib.pyplot as plt

import seaborn as sns

from matplotlib import gridspec

Now we read the data and try to understand each feature's meaning. The Python module [pandas](https://pandas.pydata.org/) provide us with the functions to read data. In the next step, we will read the data from our directory where the data is saved, and then we look at the first and last five rows of the data using head(), and tail() methods:

dataset = pd.read\_csv("creditcard.csv")

dataset.head().append(dataset.tail())

╔════════╤══════════╤════════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤════════╤═══════╗

║ │ Time │ V1 │ V2 │ V3 │ V4 │ V5 │ V6 │ V7 │ V8 │ V9 │ ... │ V21 │ V22 │ V23 │ V24 │ V25 │ V26 │ V27 │ V28 │ Amount │ Class ║

╠════════╪══════════╪════════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪════════╪═══════╣

║ 0 │ 0.0 │ -1.359807 │ -0.072781 │ 2.536347 │ 1.378155 │ -0.338321 │ 0.462388 │ 0.239599 │ 0.098698 │ 0.363787 │ ... │ -0.018307 │ 0.277838 │ -0.110474 │ 0.066928 │ 0.128539 │ -0.189115 │ 0.133558 │ -0.021053 │ 149.62 │ 0 ║

╟────────┼──────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼────────┼───────╢

║ 1 │ 0.0 │ 1.191857 │ 0.266151 │ 0.166480 │ 0.448154 │ 0.060018 │ -0.082361 │ -0.078803 │ 0.085102 │ -0.255425 │ ... │ -0.225775 │ -0.638672 │ 0.101288 │ -0.339846 │ 0.167170 │ 0.125895 │ -0.008983 │ 0.014724 │ 2.69 │ 0 ║

╟────────┼──────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼────────┼───────╢

║ 2 │ 1.0 │ -1.358354 │ -1.340163 │ 1.773209 │ 0.379780 │ -0.503198 │ 1.800499 │ 0.791461 │ 0.247676 │ -1.514654 │ ... │ 0.247998 │ 0.771679 │ 0.909412 │ -0.689281 │ -0.327642 │ -0.139097 │ -0.055353 │ -0.059752 │ 378.66 │ 0 ║

╟────────┼──────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼────────┼───────╢

║ 3 │ 1.0 │ -0.966272 │ -0.185226 │ 1.792993 │ -0.863291 │ -0.010309 │ 1.247203 │ 0.237609 │ 0.377436 │ -1.387024 │ ... │ -0.108300 │ 0.005274 │ -0.190321 │ -1.175575 │ 0.647376 │ -0.221929 │ 0.062723 │ 0.061458 │ 123.50 │ 0 ║

╟────────┼──────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼────────┼───────╢

║ 4 │ 2.0 │ -1.158233 │ 0.877737 │ 1.548718 │ 0.403034 │ -0.407193 │ 0.095921 │ 0.592941 │ -0.270533 │ 0.817739 │ ... │ -0.009431 │ 0.798278 │ -0.137458 │ 0.141267 │ -0.206010 │ 0.502292 │ 0.219422 │ 0.215153 │ 69.99 │ 0 ║

╟────────┼──────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼────────┼───────╢

║ 284802 │ 172786.0 │ -11.881118 │ 10.071785 │ -9.834783 │ -2.066656 │ -5.364473 │ -2.606837 │ -4.918215 │ 7.305334 │ 1.914428 │ ... │ 0.213454 │ 0.111864 │ 1.014480 │ -0.509348 │ 1.436807 │ 0.250034 │ 0.943651 │ 0.823731 │ 0.77 │ 0 ║

╟────────┼──────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼────────┼───────╢

║ 284803 │ 172787.0 │ -0.732789 │ -0.055080 │ 2.035030 │ -0.738589 │ 0.868229 │ 1.058415 │ 0.024330 │ 0.294869 │ 0.584800 │ ... │ 0.214205 │ 0.924384 │ 0.012463 │ -1.016226 │ -0.606624 │ -0.395255 │ 0.068472 │ -0.053527 │ 24.79 │ 0 ║

╟────────┼──────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼────────┼───────╢

║ 284804 │ 172788.0 │ 1.919565 │ -0.301254 │ -3.249640 │ -0.557828 │ 2.630515 │ 3.031260 │ -0.296827 │ 0.708417 │ 0.432454 │ ... │ 0.232045 │ 0.578229 │ -0.037501 │ 0.640134 │ 0.265745 │ -0.087371 │ 0.004455 │ -0.026561 │ 67.88 │ 0 ║

╟────────┼──────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼────────┼───────╢

║ 284805 │ 172788.0 │ -0.240440 │ 0.530483 │ 0.702510 │ 0.689799 │ -0.377961 │ 0.623708 │ -0.686180 │ 0.679145 │ 0.392087 │ ... │ 0.265245 │ 0.800049 │ -0.163298 │ 0.123205 │ -0.569159 │ 0.546668 │ 0.108821 │ 0.104533 │ 10.00 │ 0 ║

╟────────┼──────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼────────┼───────╢

║ 284806 │ 172792.0 │ -0.533413 │ -0.189733 │ 0.703337 │ -0.506271 │ -0.012546 │ -0.649617 │ 1.577006 │ -0.414650 │ 0.486180 │ ... │ 0.261057 │ 0.643078 │ 0.376777 │ 0.008797 │ -0.473649 │ -0.818267 │ -0.002415 │ 0.013649 │ 217.00 │ 0 ║

╚════════╧══════════╧════════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧════════╧═══════╝

The Time is measured in seconds since the first transaction in the data collection. As a result, we may infer that this dataset contains all transactions recorded during two days. The features were prepared using PCA, so the physical interpretation of individual features does not make sense. 'Time' and 'Amount' are the only features that are not transformed to PCA. 'Class' is the response variable, and it has a value of 1 if there is fraud and 0 otherwise.

## Data Exploration and Visualization

Now we try to find out the relative proportion of valid and fraudulent credit card transactions:

print("Fraudulent Cases: " + str(len(dataset[dataset["Class"] == 1])))

print("Valid Transactions: " + str(len(dataset[dataset["Class"] == 0])))

print("Proportion of Fraudulent Cases: " + str(len(dataset[dataset["Class"] == 1])/ dataset.shape[0]))

data\_p = dataset.copy()

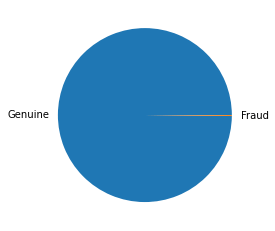
data\_p[" "] = np.where(data\_p["Class"] == 1 , "Fraud", "Genuine")

data\_p[" "].value\_counts().plot(kind="pie")

Fraudulent Cases: 492

Valid Transactions: 284315

Proportion of Fraudulent Cases: 0.001727485630620034



There is an imbalance in the data, with only 0.17% of the total cases being fraudulent.

Now we look at the distribution of the two named features in the dataset. For Time, it is clear that there was a particular duration in the day when most of the transactions took place:

f, axes = plt.subplots(1, 2, figsize=(18,4), sharex = True)

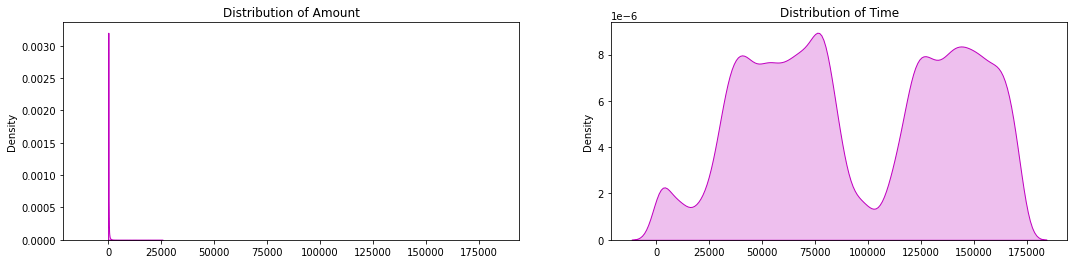
amount\_value = dataset['Amount'].values # values

time\_value = dataset['Time'].values # values

sns.distplot(amount\_value, hist=False, color="m", kde\_kws={"shade": True}, ax=axes[0]).set\_title('Distribution of Amount')

sns.distplot(time\_value, hist=False, color="m", kde\_kws={"shade": True}, ax=axes[1]).set\_title('Distribution of Time')

plt.show()



Let us check if there is any difference between valid transactions and fraudulent transactions:

print("Average Amount in a Fraudulent Transaction: " + str(dataset[dataset["Class"] == 1]["Amount"].mean()))

print("Average Amount in a Valid Transaction: " + str(dataset[dataset["Class"] == 0]["Amount"].mean()))

Average Amount in a Fraudulent Transaction: 122.21132113821133

Average Amount in a Valid Transaction: 88.29102242225574

As we can notice from this, the average money transaction for the fraudulent ones is more. It makes this problem crucial to deal with. Now let us try to understand the distribution of values in each feature. Let's start with the Amount:

print("Summary of the feature - Amount" + "\n-------------------------------")

print(dataset["Amount"].describe())

Summary of the feature - Amount

-------------------------------

count 284807.000000

mean 88.349619

std 250.120109

min 0.000000

25% 5.600000

50% 22.000000

75% 77.165000

max 25691.160000

Name: Amount, dtype: float64

The rest of the features don't have any physical interpretation and will be seen through histograms. Here the values are subgrouped according to class (valid or fraud):

data\_plot = dataset.copy()

amount = data\_plot['Amount']

data\_plot.drop(labels=['Amount'], axis=1, inplace = True)

data\_plot.insert(0, 'Amount', amount)

columns = data\_plot.iloc[:,0:30].columns

plt.figure(figsize=(12,30\*4))

grids = gridspec.GridSpec(30, 1)

for grid, index in enumerate(data\_plot[columns]):

ax = plt.subplot(grids[grid])

sns.distplot(data\_plot[index][data\_plot.Class == 1], hist=False, kde\_kws={"shade": True}, bins=50)

sns.distplot(data\_plot[index][data\_plot.Class == 0], hist=False, kde\_kws={"shade": True}, bins=50)

ax.set\_xlabel("")

ax.set\_title("Distribution of Column: " + str(index))

plt.show()

Some common data processing tasks include:

Credit card fraud detection involves a range of data processing tasks to identify and prevent fraudulent transactions. Here are some common data processing tasks in credit card fraud detection:

1. Data Collection:
   * Acquiring transaction data from various sources, including point-of-sale terminals, online payment gateways, and mobile applications.
2. Data Preprocessing:
   * Data cleaning to handle missing or inconsistent data.
   * Data transformation, such as normalizing or standardizing features.
   * Feature engineering to create new variables that may aid in fraud detection.
3. Data Integration:
   * Combining transaction data from multiple sources to create a comprehensive dataset.
4. Data Sampling:
   * Creating a balanced dataset by undersampling the majority class (legitimate transactions) or oversampling the minority class (fraudulent transactions) to avoid class imbalance issues.
5. Data Splitting:
   * Splitting the dataset into training, validation, and testing sets for model development and evaluation.
6. Exploratory Data Analysis (EDA):
   * Exploring the data to understand its distribution, patterns, and relationships.
   * Visualizing transaction statistics, such as transaction amounts, timestamps, and card usage.
7. Feature Selection:
   * Identifying and selecting the most relevant features for the model to reduce dimensionality and improve model performance.
8. Model Training:
   * Building and training machine learning models, such as logistic regression, decision trees, random forests, or deep learning models like neural networks.
   * Hyperparameter tuning to optimize model performance.
9. Anomaly Detection:
   * Applying anomaly detection techniques to identify unusual or suspicious patterns in transactions.
10. Real-time Monitoring:
    * Processing incoming transaction data in real-time to detect and flag potentially fraudulent transactions as they occur.
11. Model Evaluation:
    * Assessing model performance using metrics like accuracy, precision, recall, F1-score, and ROC AUC.
    * Cross-validation to ensure model robustness.
12. Threshold Optimization:
    * Setting decision thresholds to balance false positives and false negatives, depending on the desired level of fraud detection and false positive tolerance.
13. Post-processing:
    * Applying additional post-processing techniques to further refine model predictions, like clustering or outlier removal.
14. Reporting and Alerting:
    * Generating alerts and reports for transactions suspected of fraud for manual review by fraud analysts.
15. Continuous Improvement:
    * Regularly retraining and updating models to adapt to evolving fraud patterns and minimize false positives.
16. Data Storage and Archiving:
    * Storing historical transaction data for auditing, compliance, and future analysis.
17. Compliance:
    * Ensuring that the data processing and fraud detection processes comply with relevant regulations, such as GDPR or PCI DSS.

These data processing tasks play a crucial role in building effective credit card fraud detection systems that can protect cardholders and financial institutions from fraudulent activities.

How to overcome the challenges of loading and preprocessing a

detection dataset:

There are a number of things that can be done to overcome the

challenges of loading and preprocessing a house price dataset, including:

 Use a data preprocessing library:

There are a number of libraries available that can help with data

preprocessing tasks, such as handling missing values, encoding

categorical variables, and scaling the features.

 Carefully consider the specific needs of your model:

The best way to preprocess the data will depend on the specific

machine learning algorithm that you are using. It is important to

carefully consider the requirements of the algorithm and to preprocess

the data in a way that is compatible with the algorithm.

 Validate the preprocessed data:

It is important to validate the preprocessed data to ensure that it is

in a format that can be used by the machine learning algorithm and that

it is of high quality. This can be done by inspecting the data visually or

by using statistical methods.

 Data preprocessing is the process of cleaning, transforming, and

integrating data in order to make it ready for analysis.

 This may involve removing errors and inconsistencies, handling

missing values, transforming the data into a consistent format, and

scaling the data to a suitable range.

Certainly, let's delve into the development phase of credit card fraud detection in even more detail:

Data Collection and Preprocessing:

Data Gathering:

Collect historical transaction data, which may span several years. This data should include various attributes like transaction amount, time, location, merchant information, and cardholder details.

Data Sources:

Data can come from a variety of sources, including internal records, payment processors, and industry databases.

Data Sampling:

Depending on the size of the dataset, it might be necessary to take a random or stratified sample to manage computational resources effectively.

Data Cleaning and Transformation:

Data Cleaning:

Address issues such as missing values, outliers, and inconsistencies. This may involve imputing missing values, removing duplicates, and correcting erroneous entries.

Data Transformation:

Normalize or standardize numerical features to ensure that they are on the same scale. Categorical data may need to be one-hot encoded.

Time-based features may require feature engineering to extract relevant information, like day of the week or hour of the day.

Exploratory Data Analysis (EDA):

Conduct thorough EDA to gain insights into the data, understand the distribution of features, and identify potential patterns or anomalies that could be indicative of fraud.

Feature Engineering:

Feature Selection:

Use domain knowledge and statistical tests to select the most relevant features for fraud detection.

Feature Creation:

Generate new features that capture relationships or patterns in the data, such as aggregations, ratios, or time-based features.

Feature Scaling:

Apply scaling methods like Standardization (Z-score scaling) to numerical features.

Data Splitting:

Stratified Sampling:

Ensure that the training, validation, and test datasets have a balanced representation of both legitimate and fraudulent transactions.

Time-Based Split:

When dealing with chronological data, split the data based on time, ensuring that the model is tested on more recent data.

Model Selection:

Consider a variety of models including:

Logistic Regression

Decision Trees

Random Forests

Support Vector Machines

Neural Networks

Gradient Boosting Algorithms (XGBoost, LightGBM)

Experiment with ensemble methods for combining the strengths of multiple models.

Model Training:

Train the chosen model(s) on the training dataset using an appropriate loss function (e.g., binary cross-entropy for binary classification).

Hyperparameter Tuning:

Use techniques like grid search, random search, or Bayesian optimization to find the optimal hyperparameters for each model.

Model Evaluation:

Evaluate model performance on the validation dataset using various metrics, including but not limited to:

Accuracy

Precision

Recall

F1 Score

ROC-AUC

Generate a confusion matrix to understand the model's performance in terms of true positives, true negatives, false positives, and false negatives.

Threshold Selection:

Choose an appropriate threshold for the model's prediction probabilities to classify transactions as legitimate or fraudulent. The choice may involve considering business needs, such as minimizing false positives or maximizing true positives.

Model Deployment:

Deploy the trained model into a production environment where it can process real-time credit card transactions.

Implement necessary infrastructure for low-latency predictions and scalability.

Monitoring and Alerts:

Implement real-time monitoring of the fraud detection system and set up alerts for suspicious patterns or system failures.

Continuously analyze model drift and retrain the model as needed.

Feedback Loop:

Collect and incorporate feedback from fraud analysts and investigators to improve the model's performance and adapt to evolving fraud tactics.

Integration with Fraud Prevention Tools:

Integrate the fraud detection system with other security measures, such as two-factor authentication, biometric authentication, and real-time SMS or email notifications for cardholders.

Compliance and Reporting:

Ensure that the fraud detection system complies with legal and regulatory requirements (e.g., GDPR, PCI DSS).

Maintain detailed audit logs and reporting capabilities to track transactions and model performance.

User Education and Communication:

Educate cardholders about the importance of safeguarding their card information and teach them to recognize and report potential fraud.

Establish channels for customers to report suspicious transactions.

The development phase of credit card fraud detection is a complex and ongoing process that requires constant vigilance and adaptation to new fraud techniques. The quality of data, the choice of algorithms, and the effectiveness of monitoring are all critical factors in building a robust fraud detection system.

Key Features and Components:

Input Layer:

FraudGuard takes a wide range of transaction attributes as input, which may include:

Transaction amount

Transaction date and time

Merchant information (e.g., merchant category, location)

Cardholder information (e.g., card type, country)

Historical transaction behavior (e.g., card usage patterns)

Additional features derived from feature engineering

Feature Engineering:

Before input, the model processes data through a feature engineering pipeline to create new features and transform the raw data into a suitable format for analysis.

This may involve normalizing numerical features, one-hot encoding categorical features, and extracting time-based features.

Model Architecture:

FraudGuard employs a gradient boosting ensemble model, specifically XGBoost.

It consists of an ensemble of decision trees that work together to make predictions. Each tree learns different aspects of the data, and their predictions are combined to make a final decision.

XGBoost is chosen for its ability to handle imbalanced datasets and adapt to changing patterns in fraud.

Training:

FraudGuard is trained on a historical dataset of credit card transactions, which includes both legitimate and fraudulent examples.

The model learns to distinguish between the two classes by optimizing a binary cross-entropy loss function during the training process.

Hyperparameter tuning is employed to find the best model configuration.

Threshold Setting:

After training, a decision threshold is set to classify transactions as either legitimate or fraudulent. The threshold can be adjusted to achieve a balance between minimizing false positives and false negatives, depending on the risk tolerance of the financial institution.

Real-time Prediction:

FraudGuard is deployed in a real-time processing environment, where it evaluates incoming credit card transactions as they occur.

For each transaction, it computes a probability score indicating the likelihood of fraud.

Alert System:

When a transaction is flagged as potentially fraudulent (i.e., the probability score exceeds the threshold), the system generates an alert for further investigation.

These alerts are sent to fraud analysts or cardholders, depending on the situation, allowing for timely action.

Feedback Loop:

The model continuously collects feedback from analysts and investigators to improve its performance and adapt to new fraud tactics.

Periodic retraining is scheduled to ensure the model remains up-to-date.

Evaluation and Performance Metrics:

FraudGuard's performance is assessed using various evaluation metrics, including:

Accuracy

Precision

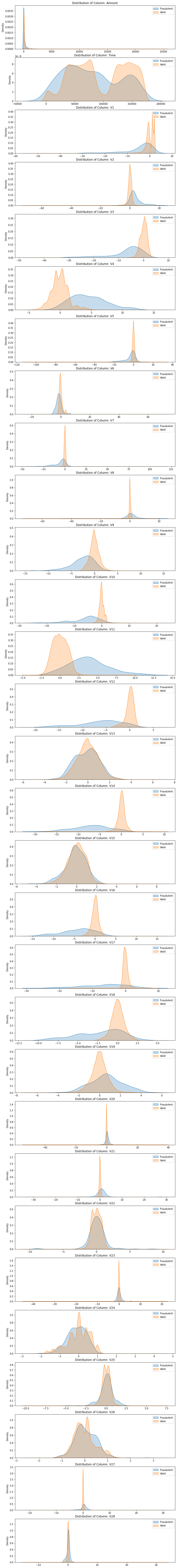
Recall

F1 Score

ROC-AUC

These metrics are monitored to ensure the model maintains a balance between minimizing false positives (legitimate transactions incorrectly classified as fraud) and false negatives (fraudulent transactions not detected).

FraudGuard is a robust and adaptive model that helps financial institutions protect their customers from credit card fraud while minimizing disruptions to legitimate transactions. Its performance and effectiveness are continuously monitored and improved to stay ahead of evolving fraud tactics and maintain high levels of security.



Importance of loading and processing dataset:

Loading and processing datasets is a critical step in many data-driven tasks, especially in the fields of machine learning, data analysis, and artificial intelligence. The importance of this step can be summarized as follows:

1. **Data Quality Assurance:** Loading and processing datasets allow you to examine and clean the data. This is crucial because real-world data is often messy, containing missing values, outliers, and errors. Data preprocessing helps ensure the quality and reliability of the data used for analysis or modeling.
2. **Feature Engineering:** Processing data involves selecting relevant features and transforming them into a suitable format. Proper feature selection and engineering can significantly impact the performance of machine learning models. This step is critical for enhancing the predictive power of models.
3. **Normalization and Standardization:** Data preprocessing often includes techniques like normalization and standardization, which can make the data more suitable for various machine learning algorithms. This step helps ensure that the scales of different features are comparable.
4. **Dimensionality Reduction:** High-dimensional data can be challenging to work with. Dimensionality reduction techniques, like Principal Component Analysis (PCA) or feature selection, help reduce the number of features while retaining the most critical information. This can lead to faster training times and better model performance.
5. **Data Integration:** In many cases, data comes from various sources and in different formats. Loading and processing data enable you to integrate diverse datasets and prepare them for analysis or modeling. This is essential for holistic insights and decision-making.
6. **Data Understanding:** As you load and process a dataset, you gain a better understanding of its characteristics, such as the distribution of values, statistical properties, and relationships between variables. This understanding is crucial for choosing appropriate algorithms and making informed decisions.
7. **Data Visualization:** Preprocessing often includes data visualization, which helps you identify patterns, trends, and correlations in the data. Visualizing the data can provide insights that guide subsequent analysis and modeling tasks.
8. **Computational Efficiency:** Efficient data processing can significantly reduce the time and resources required for training machine learning models. Properly processed data can lead to faster convergence and reduced computational costs.
9. **Model Performance:** The quality of data preprocessing can directly impact the performance of machine learning models. Well-preprocessed data can lead to more accurate, robust, and interpretable models.
10. **Ethical Considerations:** Data preprocessing also plays a role in addressing ethical and privacy concerns. It includes steps to anonymize or de-identify sensitive information and ensure that models are not biased or discriminatory.

In summary, loading and processing datasets are foundational steps in the data analysis and machine learning pipeline. The quality and effectiveness of these steps can have a profound impact on the success of data-driven projects, making them crucial for extracting valuable insights, making informed decisions, and building accurate predictive models.

## Data Preparation

Since the features are created using PCA, feature selection is unnecessary as many features are tiny. Let's see if there are any missing values in the dataset:

dataset.isnull().shape[0]

print("Non-missing values: " + str(dataset.isnull().shape[0]))

print("Missing values: " + str(dataset.shape[0] - dataset.isnull().shape[0]))

Non-missing values: 284807

Missing values: 0

As there are no missing data, we turn to standardization. We standardize only Time and Amount using [RobustScaler](https://scikit-learn.org/stable/modules/generated/sklearn.preprocessing.RobustScaler.html" \o "RobustScaler" \t "_blank):

from sklearn.preprocessing import RobustScaler

scaler = RobustScaler().fit(dataset[["Time", "Amount"]])

dataset[["Time", "Amount"]] = scaler.transform(dataset[["Time", "Amount"]])

dataset.head().append(dataset.tail())

As we saw previously, the Amount column has outliers, that's why we chose RobustScaler() as it's robust to outliers. Output:

╔════════╤═══════════╤════════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════════╤═══════╗

║ │ Time │ V1 │ V2 │ V3 │ V4 │ V5 │ V6 │ V7 │ V8 │ V9 │ ... │ V21 │ V22 │ V23 │ V24 │ V25 │ V26 │ V27 │ V28 │ Amount │ Class ║

╠════════╪═══════════╪════════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════════╪═══════╣

║ 0 │ -0.994983 │ -1.359807 │ -0.072781 │ 2.536347 │ 1.378155 │ -0.338321 │ 0.462388 │ 0.239599 │ 0.098698 │ 0.363787 │ ... │ -0.018307 │ 0.277838 │ -0.110474 │ 0.066928 │ 0.128539 │ -0.189115 │ 0.133558 │ -0.021053 │ 1.783274 │ 0 ║

╟────────┼───────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────╢

║ 1 │ -0.994983 │ 1.191857 │ 0.266151 │ 0.166480 │ 0.448154 │ 0.060018 │ -0.082361 │ -0.078803 │ 0.085102 │ -0.255425 │ ... │ -0.225775 │ -0.638672 │ 0.101288 │ -0.339846 │ 0.167170 │ 0.125895 │ -0.008983 │ 0.014724 │ -0.269825 │ 0 ║

╟────────┼───────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────╢

║ 2 │ -0.994972 │ -1.358354 │ -1.340163 │ 1.773209 │ 0.379780 │ -0.503198 │ 1.800499 │ 0.791461 │ 0.247676 │ -1.514654 │ ... │ 0.247998 │ 0.771679 │ 0.909412 │ -0.689281 │ -0.327642 │ -0.139097 │ -0.055353 │ -0.059752 │ 4.983721 │ 0 ║

╟────────┼───────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────╢

║ 3 │ -0.994972 │ -0.966272 │ -0.185226 │ 1.792993 │ -0.863291 │ -0.010309 │ 1.247203 │ 0.237609 │ 0.377436 │ -1.387024 │ ... │ -0.108300 │ 0.005274 │ -0.190321 │ -1.175575 │ 0.647376 │ -0.221929 │ 0.062723 │ 0.061458 │ 1.418291 │ 0 ║

╟────────┼───────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────╢

║ 4 │ -0.994960 │ -1.158233 │ 0.877737 │ 1.548718 │ 0.403034 │ -0.407193 │ 0.095921 │ 0.592941 │ -0.270533 │ 0.817739 │ ... │ -0.009431 │ 0.798278 │ -0.137458 │ 0.141267 │ -0.206010 │ 0.502292 │ 0.219422 │ 0.215153 │ 0.670579 │ 0 ║

╟────────┼───────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────╢

║ 284802 │ 1.034951 │ -11.881118 │ 10.071785 │ -9.834783 │ -2.066656 │ -5.364473 │ -2.606837 │ -4.918215 │ 7.305334 │ 1.914428 │ ... │ 0.213454 │ 0.111864 │ 1.014480 │ -0.509348 │ 1.436807 │ 0.250034 │ 0.943651 │ 0.823731 │ -0.296653 │ 0 ║

╟────────┼───────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────╢

║ 284803 │ 1.034963 │ -0.732789 │ -0.055080 │ 2.035030 │ -0.738589 │ 0.868229 │ 1.058415 │ 0.024330 │ 0.294869 │ 0.584800 │ ... │ 0.214205 │ 0.924384 │ 0.012463 │ -1.016226 │ -0.606624 │ -0.395255 │ 0.068472 │ -0.053527 │ 0.038986 │ 0 ║

╟────────┼───────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────╢

║ 284804 │ 1.034975 │ 1.919565 │ -0.301254 │ -3.249640 │ -0.557828 │ 2.630515 │ 3.031260 │ -0.296827 │ 0.708417 │ 0.432454 │ ... │ 0.232045 │ 0.578229 │ -0.037501 │ 0.640134 │ 0.265745 │ -0.087371 │ 0.004455 │ -0.026561 │ 0.641096 │ 0 ║

╟────────┼───────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────╢

║ 284805 │ 1.034975 │ -0.240440 │ 0.530483 │ 0.702510 │ 0.689799 │ -0.377961 │ 0.623708 │ -0.686180 │ 0.679145 │ 0.392087 │ ... │ 0.265245 │ 0.800049 │ -0.163298 │ 0.123205 │ -0.569159 │ 0.546668 │ 0.108821 │ 0.104533 │ -0.167680 │ 0 ║

╟────────┼───────────┼────────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼─────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────────┼───────╢

║ 284806 │ 1.035022 │ -0.533413 │ -0.189733 │ 0.703337 │ -0.506271 │ -0.012546 │ -0.649617 │ 1.577006 │ -0.414650 │ 0.486180 │ ... │ 0.261057 │ 0.643078 │ 0.376777 │ 0.008797 │ -0.473649 │ -0.818267 │ -0.002415 │ 0.013649 │ 2.724796 │ 0 ║

╚════════╧═══════════╧════════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════════╧═══════╝

10 rows × 31 columns

Next, let's divide the data into features and targets. We also make the train-test split of the data:

y = dataset["Class"] # target

X = dataset.iloc[:,0:30]

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

X\_train, X\_test, y\_train, y\_test = train\_test\_split(

X, y, test\_size = 0.2, random\_state = 42)

X\_train.shape, X\_test.shape, y\_train.shape, y\_test.shape

Output:

((227845, 30), (56962, 30), (227845,), (56962,))

Let's import all the necessary libraries for the tutorial:

from sklearn.model\_selection import StratifiedKFold

from sklearn.model\_selection import GridSearchCV, cross\_val\_score, RandomizedSearchCV

kf = StratifiedKFold(n\_splits=5, random\_state = None, shuffle = False)

from imblearn.pipeline import make\_pipeline ## Create a Pipeline using the provided estimators .

from imblearn.under\_sampling import NearMiss ## perform Under-sampling based on NearMiss methods.

from imblearn.over\_sampling import SMOTE ## PerformOver-sampling class that uses SMOTE.

from sklearn.metrics import roc\_curve, roc\_auc\_score, accuracy\_score, recall\_score, precision\_score, f1\_score

from sklearn.linear\_model import LogisticRegression

from sklearn.svm import SVC

from sklearn.neighbors import KNeighborsClassifier

from sklearn.tree import DecisionTreeClassifier

from sklearn.ensemble import RandomForestClassifier

# Model Interpretability:

Credit card fraud is a growing problem in the financial industry, with the potential to cause significant

financial losses to both customers and financial institutions. As a result, there has been a significant

amount of research in recent years on developing effective fraud detection systems. These systems rely on

a combination of statistical techniques, machine learning algorithms, and deep learning models to identify

fraudulent transactions.One of the most commonly used approaches for credit card fraud detection is

rule-based systems. These systems use predefined rules to identify transactions that are deemed suspicious.

However, rule-based systems have limitations, as they are only as good as the rules that have been

predefined, and they may not be able to detect new types of fraud. To overcome these limitations, machine

learning algorithms and statistical techniques have been applied to credit card fraud detection. These

techniques are based on analysing transaction-related data, such as the transaction amount, location, and

time, as well as other relevant factors, such as the customer’s transaction history and account details. In

recent years, deep learning models, such as convolutional neural networks (CNNs) and recurrent neural

networks (RNNs), have also been applied to credit card fraud detection. These models have shown

promising results in identifying fraudulent transactions by learning patterns in the data and improving the

accuracy of fraud detection. Overall, credit card fraud detection is a critical area of research in the financial

industry, with significant potential for improving fraud detection rates and reducing financial losse

Credit card fraud is a growing problem in the financial industry, with the potential to cause significant

financial losses to both customers and financial institutions. As a result, there has been a significant

amount of research in recent years on developing effective fraud detection systems. These systems rely on

a combination of statistical techniques, machine learning algorithms, and deep learning models to identify

fraudulent transactions.One of the most commonly used approaches for credit card fraud detection is

rule-based systems. These systems use predefined rules to identify transactions that are deemed suspicious.

However, rule-based systems have limitations, as they are only as good as the rules that have been

predefined, and they may not be able to detect new types of fraud. To overcome these limitations, machine

learning algorithms and statistical techniques have been applied to credit card fraud detection. These

techniques are based on analysing transaction-related data, such as the transaction amount, location, and

time, as well as other relevant factors, such as the customer’s transaction history and account details. In

recent years, deep learning models, such as convolutional neural networks (CNNs) and recurrent neural

networks (RNNs), have also been applied to credit card fraud detection. These models have shown

promising results in identifying fraudulent transactions by learning patterns in the data and improving the

accuracy of fraud detection. Overall, credit card fraud detection is a critical area of research in the financial

industry, with significant potential for improving fraud detection rates and reducing financial losse

Credit Card Fraud can be defined as a case where a person uses someone else’s credit card for personal reasons while the owner and the card-issuing authorities are unaware of the fact that the card is being used. Due to the rise and acceleration of E-Commerce, there has been a tremendous use of credit cards for online shopping which led to High amount of frauds related to credit cards. In the era of digitalization, the need to identify credit card frauds is necessary. Fraud detection involves monitoring and analyzing the behaviour of various users to estimate detect or avoid undesirable behaviour. To identify credit card fraud detection effectively, we need to understand the various technologies, algorithms and types involved in detecting credit card frauds. The algorithm can differentiate transactions which are fraudulent or not. Find fraud, they need to passed dataset and knowledge of the fraudulent transaction. They analyze the dataset and classify all transactions. Fraud detection involves monitoring the activities of populations of users to estimate, perceive or avoid objectionable behaviour, which consist of fraud, intrusion, and defaulting. Machine learning algorithms are employed to analyses all the authorized transactions and report the suspicious ones. These reports are investigated by professionals who contact the cardholders to confirm if the transaction was genuine or fraudulent. The investigators provide feedback to the automated system which is used to train and update the algorithm to eventually improve the fraud-detection performance over time.

Conclusion and Future Work (Phase 2)

# Project Conclusion:

In the Phase 2 conclusion: Recap Key Points: Stress the importance of fraud detection form financial security.Emphasize the Ongoing Need for Vigilance: Highlight that fraud prevention is an evolving process

Future Work: we need credit card fraud detection techniques**to protect the cardholders from false activity.** India is on its way to becoming a developed country. To achieve this, the Government of India (GoI) has launched several initiatives and one of these is Digital India Campaign. .