|  |  |
| --- | --- |
| credit card fraud detection  ADS PHASE 3 | Abstract  This paper is Phase 3 of Alok Mandal "Credit Card Fraud Detection" project, which he presented as a third-year Computer Science And Engineering student. Phase 3 is dubbed "Development Part 1," and it consists of preparing the dataset, ingesting data, doing data transformation, and starting the initial data analysis.  Alok Mandal  Applied Data Science |

* **Table of Contents:**
  + **1. Introduction**
    - **1.1 Purpose**
    - **1.2 Scope**
    - **1.3 Overview of Credit Card Fraud Detection**
  + **2. Data Preparation**
    - **2.1 Data Collection**
    - **2.2 Data Preprocessing**
      * **2.2.1 Data Cleaning**
      * **2.2.2 Feature Selection**
      * **2.2.3 Data Scaling**
      * **2.2.4 Handling Imbalanced Data**
    - **2.3 Data Splitting (Training and Testing Sets)**
  + **3. Feature Engineering**
    - **3.1 Feature Selection**
    - **3.2 Feature Transformation**
    - **3.3 Feature Scaling**
  + **4. Building a Fraud Detection Model**
    - **4.1 Selection of Machine Learning Algorithms**
      * **4.1.2 Random Forest**
      * **4.1.3 Support Vector Machine**
      * **4.1.4 Neural Network**
    - **4.2 Model Training**
    - **4.3 Model Evaluation**
      * **4.3.1 Confusion Matrix**
      * **4.3.2 Precision, Recall, and F1-Score**
      * **4.3.3 ROC Curve and AUC**
      * **4.3.4 Cross-Validation**
  + **5. Hyperparameter Tuning**
    - **5.1 Grid Search**
    - **5.2 Random Search**
    - **5.3 Hyperparameter Optimization**
  + **6. Model Deployment**
    - **6.1 Saving the Trained Model**
    - **6.2 Building an API**
    - **6.3 Real-time Fraud Detection**
  + **7. Conclusion**
    - **7.1 Summary of Results**
    - **7.2 Future Improvements**
  + **8. References**

**1. Introduction**

**1.1 Purpose**

This Python program aims to create a credit card fraud detection system that uses machine learning techniques to automatically identify and flag fraudulent transactions, enhancing security and protecting cardholders and financial institutions from fraudulent activities.

**1.2 Scope**

This project aims to develop a comprehensive credit card fraud detection system, covering data preparation, feature engineering, model building, hyperparameter tuning, and deployment, from data collection to real-time fraud detection.

**1.3 Overview of Credit Card Fraud Detection**

Credit card fraud detection is crucial for financial security, especially with the growing use of credit and debit cards. A program uses historical transaction data, machine learning algorithms, and statistical techniques to create a predictive model that can distinguish between legitimate and fraudulent transactions. The model's predictions help financial institutions and cardholders take appropriate actions to prevent losses and protect the financial system's integrity.

**2. Data Preparation**

**2.1 Data Collection**

This project collects transaction data from financial institutions, card payment processors, and publicly available datasets, including transaction amount, timestamp, card number, merchant information, and transaction outcome (fraudulent or legitimate), for data collection purposes.

**2.2 Data Preprocessing**

Data preprocessing is a crucial step to ensure the quality and suitability of the data for machine learning. This step includes several subtasks:

**2.2.1 Data Cleaning**

Data cleaning is a process that identifies and removes missing values, duplicates, and outliers from transaction datasets, ensuring data reliability and accuracy for fraud detection models.

**2.2.2 Feature Selection**

Feature selection is the process of selecting the most relevant attributes from a dataset, which can reduce data dimensionality and enhance model efficiency, including transaction-specific information like transaction amount and location.

**2.2.3 Data Scaling**

Data scaling is a technique used to normalize feature values, ensuring no single feature dominates the model's learning process. Common techniques include standardization or normalization, which ensure features have a mean of 0 and standard deviation of 1.

**2.2.4 Handling Imbalanced Data**

Imbalanced data refers to a situation where the number of legitimate transactions outweighs the number of fraudulent ones, and can be effectively handled by techniques like oversampling the minority class or under sampling the majority class.

**2.3 Data Splitting (Training and Testing Sets)**

The machine learning model's performance is evaluated by dividing the dataset into a training and testing set. The training set is used for training, while the testing set evaluates its performance on unseen data. Common splitting ratios are 70/30 or 80/20. The next sections will cover feature engineering, model building, hyperparameter tuning, and the deployment of the credit card fraud detection system.

**3. Feature Engineering**

**3.1 Feature Selection**

Feature selection is the process of selecting the most relevant features from a dataset to enhance machine learning model efficiency. In credit card fraud detection, it involves identifying transaction attributes like transaction amount, time, and merchant details that provide the most informative information for distinguishing between fraudulent and legitimate transactions.

**3.2 Feature Transformation**

Feature transformation involves altering or creating new features to make the data more suitable for the model. This step can include techniques such as:

- Encoding categorical variables: Converting categorical attributes like merchant category or card type into numerical values.

- Creating derived features: Generating new features, such as transaction hour or day of the week, based on existing data to capture temporal patterns.

- Dimensionality reduction: Reducing the number of features using techniques like Principal Component Analysis (PCA) or feature extraction.

**3.3 Feature Scaling**

Feature scaling ensures that all features have a similar scale and range, preventing some features from dominating the model's learning process. Common scaling techniques include:

- Standardization: Scaling features to have a mean of 0 and a standard deviation of 1.

- Normalization: Scaling features to a specific range, typically [0, 1] or [-1, 1].

- Min-Max scaling: Scaling features to a specified range based on their minimum and maximum values.

Proper feature engineering can significantly impact the performance of the credit card fraud detection model. In the following sections, we will delve into the process of building the fraud detection model, tuning hyperparameters, and deploying the system.

**4. Building a Fraud Detection Model**

**4.1 Selection of Machine Learning Algorithms**

In this section, we explore different machine learning algorithms for credit card fraud detection. We consider the following algorithms:

**4.1.1 Logistic Regression**

As a basis model, logistic regression is a straightforward and understandable technique. It works well for binary classification problems and can shed light on the significance of particular traits.

**4.1.2 Random Forest**

Multiple decision trees are used in Random Forest, an ensemble learning technique, to increase prediction accuracy. It can manage intricate data connections and is resistant to overfitting.

**4.1.3 Support Vector Machine**

The Support Vector Machine (SVM) is a potent binary classification technique. In order to optimize the margin between the classes, a hyperplane must be found. SVM uses kernel functions to handle non-linear data.

**4.1.4 Neural Network**

Deep learning models in particular, which use neural networks, are very flexible and capable of identifying intricate patterns in data. Large and high-dimensional dataset problems are a good fit for them.

**4.2 Model Training**

Using the preprocessed and feature-engineered data, we train the models after choosing the machine learning techniques. To discover the correlations and patterns in the data, each algorithm is trained using the training dataset.

**4.3 Model Evaluation**

To assess the performance of the fraud detection models, we employ various evaluation metrics and techniques.

**4.3.1 Confusion Matrix**

The confusion matrix is a tabulation of true positive, true negative, false positive, and false negative values, providing a detailed view of the model's performance in binary classification.

**4.3.2 Precision, Recall, and F1-Score**

Recall (sensitivity) assesses the percentage of genuine positives that are accurately detected, whereas precision is the percentage of true positive predictions among all positive predictions. The harmonic mean of recall and accuracy yields the F1-Score, a fair statistic for assessing models.

**4.3.3 ROC Curve and AUC**

The trade-off between the true positive rate and the false positive rate for various thresholds is depicted by the Receiver Operating Characteristic (ROC) curve. The model's overall performance is measured by the Area Under the Curve (AUC).

**4.3.4 Cross-Validation**

The dataset is divided into many folds and then subjected to cross-validation, which evaluates the model's performance. It lowers the chance of overfitting and helps guarantee the model's capacity for generalization.

We will examine model deployment and hyperparameter optimization for the credit card fraud detection system in the upcoming sections.

**5. Hyperparameter Tuning**

**5.1 Grid Search**

A critical step in maximizing the effectiveness of the machine learning models is hyperparameter tweaking. One method for fine-tuning hyperparameters is grid search. To discover the combination that produces the highest model performance, a preset set of hyperparameters must be methodically searched through.

**5.2 Random Search**

An alternate strategy to hyperparameter tweaking is random search. It randomly selects hyperparameters from predefined distributions, in contrast to grid search. When working with a vast hyperparameter space, random search is more effective since it can identify appropriate hyperparameter combinations faster.

**5.3 Hyperparameter Optimization**

A more general term for these kinds of methods is "hyperparameter optimization," which also includes random search, grid search, Bayesian optimization, and more. Finding the ideal hyperparameter values for a given model automatically is the aim of hyperparameter optimization. This lessens the need for human fine-tuning while also enhancing the model's performance.

We'll talk about model deployment and how to put the credit card fraud detection system into practice in the real world in the parts that follow.

**6. Model Deployment**

**6.1 Saving the Trained Model**

It is crucial to save the credit card fraud detection model to a file or storage system after it has been trained and adjusted. This makes retrieval and reuse simple. By preserving its architecture and learnt parameters, the model may be saved and used again later on without requiring retraining.

**6.2 Building an API**

An Application Programming Interface (API) is created in order to make the credit card fraud detection system usable and accessible in the real world. In order to facilitate real-time prediction queries, the API acts as a link between the model and other systems. This API offers a channel for transmitting transaction data and obtaining fraud alerts, and it may be hosted on a cloud platform or web server.

**6.3 Real-time Fraud Detection**

The credit card fraud detection system can now identify fraud in real time thanks to the API. The system has the ability to forward processed incoming transactions to the API, which utilizes the trained model to determine the likelihood of fraud in each transaction. With real-time detection, measures may be performed right away, such reporting suspicious transactions or preventing the use of possibly fraudulent cards.

We will review the findings, talk about possible enhancements in the future, and offer resources for more research in the concluding part.

**7. Conclusion**

**7.1 Summary of Results**

With the help of many machine learning algorithms, we have created a system for detecting credit card fraud for this project. Metrics including accuracy, recall, F1-score, ROC curve, and AUC have been used to assess the system's performance. The model shows that it can reliably detect fraudulent transactions and offers a useful instrument to improve credit card transaction security.

**7.2 Future Improvements**

Even if the system for detecting credit card fraud is functional and efficient, it may yet be enhanced in the future. Among the possible areas for development are:

- Including feedback systems that update in real time to accommodate changing fraud tendencies.

- Using increasingly sophisticated machine learning methods, including deep learning, to increase accuracy.

- Investigating other attributes and data sources for even more effective fraud detection.

- Using more sophisticated anomaly detection methods to identify minute fraud trends.

Improving the user interface to make it easier for cardholders and financial institutions to monitor and react to fraud warnings.

Maintaining the effectiveness of the credit card fraud detection system by ongoing monitoring, model retraining, and incremental enhancements will be crucial in the dynamic world of financial crime.

**8. References**

A list of the project's references, data sources, and resources.

We appreciate your interest in our software for detecting credit card fraud.

* **PROGRAM:-**

#preprocessing the dataset

# Naive Bayes Classification

# Importing the libraries

import numpy as np

import matplotlib.pyplot as plt

import pandas as pd

import seaborn as sns;

#Importing the dataset

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

X = dataset.iloc[:, :-1]

y = dataset.iloc[:, 30]

# Splitting the dataset into the Training set and Test set

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

X\_train, X\_test, y\_train, y\_test = train\_test\_split(X, y, test\_size = 1/3, random\_state = 2)

# Feature Scaling

from sklearn.preprocessing import StandardScaler

sc = StandardScaler()

X\_train = sc.fit\_transform(X\_train)

X\_test = sc.transform(X\_test)

# Fitting K-NN to the Training set

from sklearn.neighbors import KNeighborsClassifier

classifier = KNeighborsClassifier(n\_neighbors = 5, metric = 'minkowski', p = 2)

classifier.fit(X\_train, y\_train)

# Predicting the Training set results

y\_pred = classifier.predict(X\_train)

# Making the Confusion Matrix

from sklearn.metrics import confusion\_matrix

cm = confusion\_matrix(y\_train, y\_pred)

#Heat map of a confusion matrix

import seaborn as sns

sns.heatmap(cm,fmt=".0f",xticklabels=['CreditcardFraud\_No','CreditcardFraud\_Yes'],yticklabels=['CreditcardFraud\_No','CreditcardFraud\_Yes'],annot=True)

#sns.heatmap(cm,fmt=".0f",annot=True)

#Calculating Performance Metrics for Training Set

FP = cm.sum(axis=0) - np.diag(cm)

FN = cm.sum(axis=1) - np.diag(cm)

TP = np.diag(cm)

TN = cm.sum() - (FP + FN + TP)

FP = FP.astype(float)

FN = FN.astype(float)

TP = TP.astype(float)

TN = TN.astype(float)

# Sensitivity, hit rate, recall, or true positive rate

TPR = TP/(TP+FN)

print("Recall",TPR)

# Specificity or true negative rate

TNR = TN/(TN+FP)

print("Specificity",TNR)

# Precision or positive predictive value

PPV = TP/(TP+FP)

print("Precision",PPV)

# Negative predictive value

NPV = TN/(TN+FN)

print("Negative Predictive Value",NPV)

# Fall out or false positive rate

FPR = FP/(FP+TN)

print("False Positive Rate",FPR)

# False negative rate

FNR = FN/(TP+FN)

print("False Negative Rate",FNR)

# False discovery rate

FDR = FP/(TP+FP)

print("False Discovery Rate",FDR)

# Overall accuracy for each class

ACC = (TP+TN)/(TP+FP+FN+TN)

print("Accuracry",ACC)

# Fitting K-NN to the Testing set

from sklearn.neighbors import KNeighborsClassifier

classifier = KNeighborsClassifier(n\_neighbors = 5, metric = 'minkowski', p = 2)

classifier.fit(X\_test, y\_test)

# Predicting the Testing set results

y\_pred1 = classifier.predict(X\_test)

# Making the Confusion Matrix

from sklearn.metrics import confusion\_matrix

cm1 = confusion\_matrix(y\_test, y\_pred1)

#create an empty data frame that we have to predict

variety=pd.DataFrame()

variety['Time']=[0]

variety['V1']=[-1.3598071336738]

variety['V2']=[-0.0727811733098497]

variety['V3']=[2.53634673796914]

variety['V4']=[1.37815522427443]

variety['V5']=[-0.338320769942518]

variety['V6']=[0.462387777762292]

variety['V7']=[0.239598554061257]

variety['V8']=[0.0986979012610507]

variety['V9']=[0.363786969611213]

variety['V10']=[0.0907941719789316]

variety['V11']=[-0.551599533260813]

variety['V12']=[-0.617800855762348]

variety['V13']=[-0.991389847235408]

variety['V14']=[-0.311169353699879]

variety['V15']=[1.46817697209427]

variety['V16']=[-0.470400525259478]

variety['V17']=[0.207971241929242]

variety['V18']=[0.0257905801985591]

variety['V19']=[0.403992960255733]

variety['V20']=[0.251412098239705]

variety['V21']=[-0.018306777944153]

variety['V22']=[0.277837575558899]

variety['V23']=[-0.110473910188767]

variety['V24']=[0.0669280749146731]

variety['V25']=[0.128539358273528]

variety['V26']=[-0.189114843888824]

variety['V27']=[0.133558376740387]

variety['V28']=[-0.0210530534538215]

variety['Amount']=[149.62]

print(variety)

y\_pred1=classifier.predict(variety.values)

print("Did this transcation is Fraud:")

print(y\_pred1)