**Credit Card Fraud Detection Project**

**1. Project Overview**

The Credit Card Fraud Detection project aims to develop a robust machine learning model to identify and classify fraudulent transactions in credit card data. The project involves comprehensive data analysis, preprocessing, model selection, hyperparameter tuning, and evaluation.

**1.1 Key Objectives**

* Develop a machine learning model capable of accurately detecting fraudulent credit card transactions.
* Explore and analyse the dataset to gain insights into the distribution and patterns of legitimate and fraudulent transactions.
* Compare and evaluate the performance of logistic regression and random forest models for fraud detection.
* Ensure interpretability of the models through feature importance analysis using coefficients and SHAP values.

**\* LIBRARY USED**

* Numpy
* Pandas
* Matplotlib
* Seaborn
* Sklearn

**2. Libraries and Dependencies**

**2.1 Purpose**

This section imports the necessary Python libraries and dependencies to facilitate various data manipulation, visualization, and machine learning tasks.

**2.2 Code overview**

import numpy as np

import pandas as pd

import seaborn as sns

import matplotlib.pyplot as plt

from sklearn.model\_selection import train\_test\_split, cross\_val\_score, GridSearchCV

from sklearn.linear\_model import LogisticRegression

from sklearn.ensemble import RandomForestClassifier

from sklearn.preprocessing import StandardScaler

from sklearn.metrics import accuracy\_score, classification\_report, confusion\_matrix, roc\_auc\_score, roc\_curve

from sklearn.ensemble import IsolationForest

import warnings

warnings.filterwarnings("ignore", category=DeprecationWarning)

**Explanation:**

* NumPy and pandas: Used for efficient data manipulation & mathamatical computation of array.
* seaborn and matplotlib.pyplot: Employed for data visualization EDA purpose i used that. for better understanding of model.
* scikit-learn (sklearn): Provides tools for machine learning tasks such as model training, evaluation, prediction ,machiner learning algorithemsand, preprocessing.it will understand data and make random models and it willhelps to take decissions

warnings: Used to suppress deprecation warnings for cleaner output.

**3. Dataset Loading and Exploration**

**3.1 Purpose**

This section loads the credit card transaction dataset and explores its structure, characteristics, and potential issues.

its helps to view the data and to check sum of null vallues in columns.so we found there is no null vallue present in the data.

**3.2 Code overview**

credit\_fraud\_data = pd.read\_csv('creditcard.csv')

credit\_fraud\_data.head

credit\_fraud\_data.isnull().sum()

**4. Data Cleaning**

**4.1 Purpose**

This section identifies and addresses noisy data,data quality issues, including duplicate records.Data cleaning is the process of preparing data for analysis by removing or modifying data that is incorrect, incomplete, irrelevant, duplicated, or improperly formatted.

**4.2 Code overview**

duplicate\_rows = credit\_fraud\_data.duplicated().sum()

print('Number of duplicate records:', duplicate\_rows()

**Explanation:**

credit\_card\_data.duplicated().sum(): Calculates the number of duplicate rows.

**4.3 Class Distribution Analysis**

**4.4 Code overview**

print(credit\_fraud\_data['Class'].value\_counts())

0 284315

1 492

Name: Class, dtype: int64

**4.5 check how many columns are in the dataset.**

credit\_fraud\_data.columns

'Time', 'V1', 'V2', 'V3', 'V4', 'V5', 'V6', 'V7', 'V8', 'V9', 'V10',

'V11', 'V12', 'V13', 'V14', 'V15', 'V16', 'V17', 'V18', 'V19', 'V20',

'V21', 'V22', 'V23', 'V24', 'V25', 'V26', 'V27', 'V28', 'Amount',

'Class'

**4.6 transpose if a nice way of discribing the data ,we just need to do a,T after the dataframe and transpose show you stetistical terms above as column**

credit\_fraud\_data.describe().T

**5. Exploratory Data Analysis (EDA)**

**5.1 Purpose**

This section visualizes the data distribution and relationships among features to gain insights.

**5.2 Code overview**

**# Box plots for 'Amount' and 'Time' by class**

plt.figure(figsize=(12, 6))

sns.boxplot(x='Class', y='Amount', data=credit\_fraud\_data, showfliers=False,)

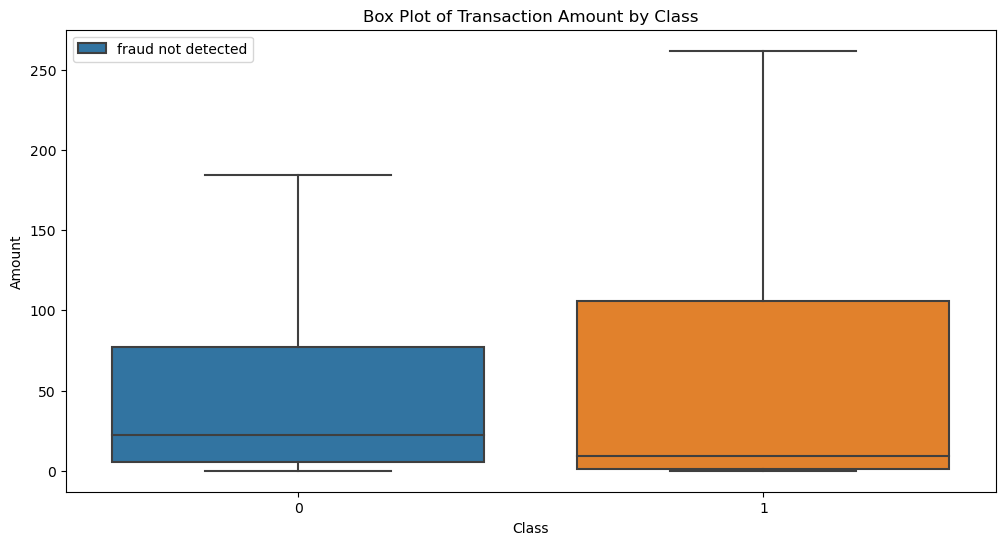
plt.title('Box Plot of Transaction Amount by Class')

plt.legend(["fraud not detected"])

plt.show()

Explaination - in this following box plot seems range between zero (0) to hundread

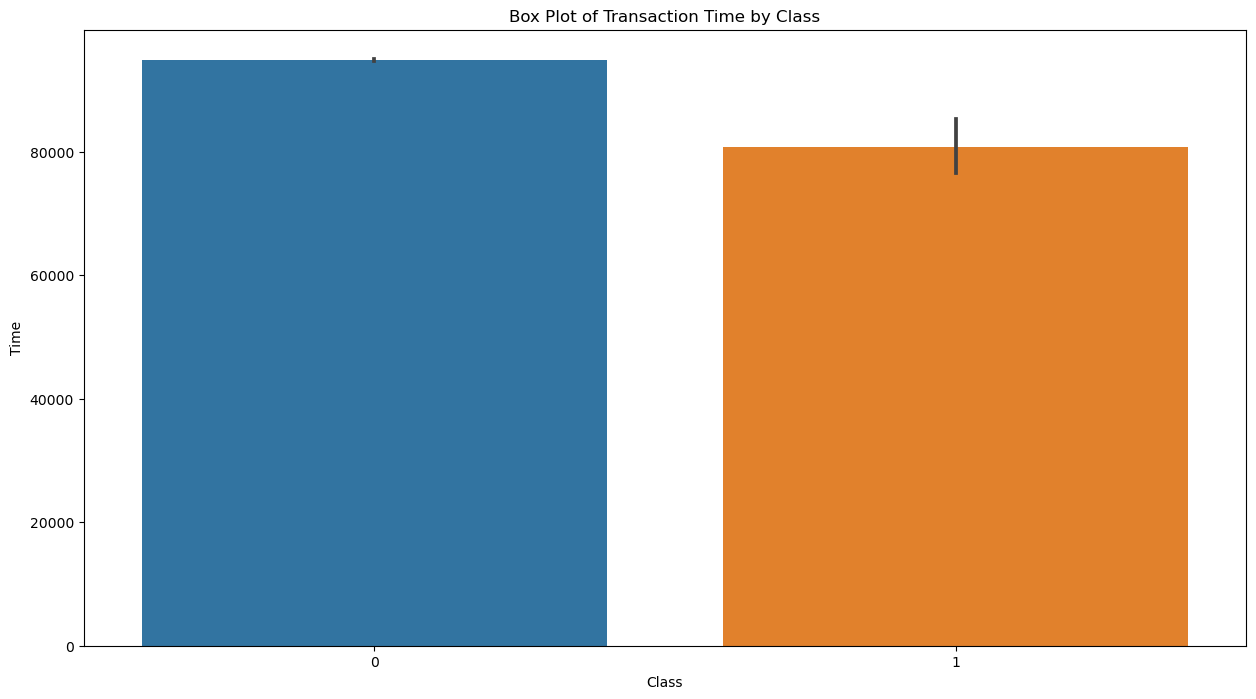
1. amount more fraud detected



plt.figure(figsize=(15,8))

sns.barplot(data=credit\_fraud\_data, y = 'Time',x='Class')

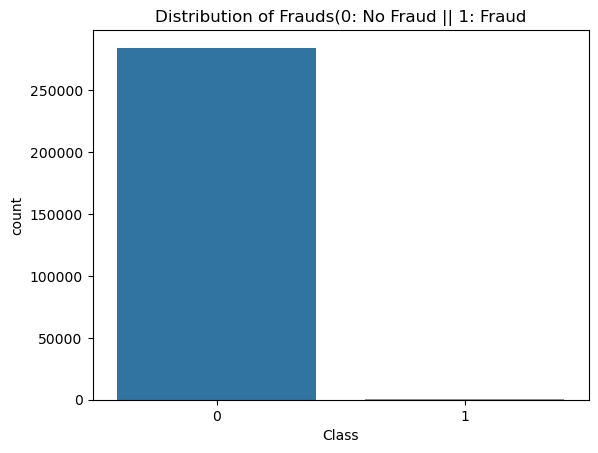
plt.title('Box Plot of Transaction Time by Class')

plt.show()

**Fraud detected and not detected bar plot**

sns.countplot(x="Class",data=credit\_fraud\_data)

plt.title('Distribution of Frauds(0: No Fraud || 1: Fraud')



**#Checking the dencity of fraud transaction amount.**

plt.figure(figsize=(12, 6))

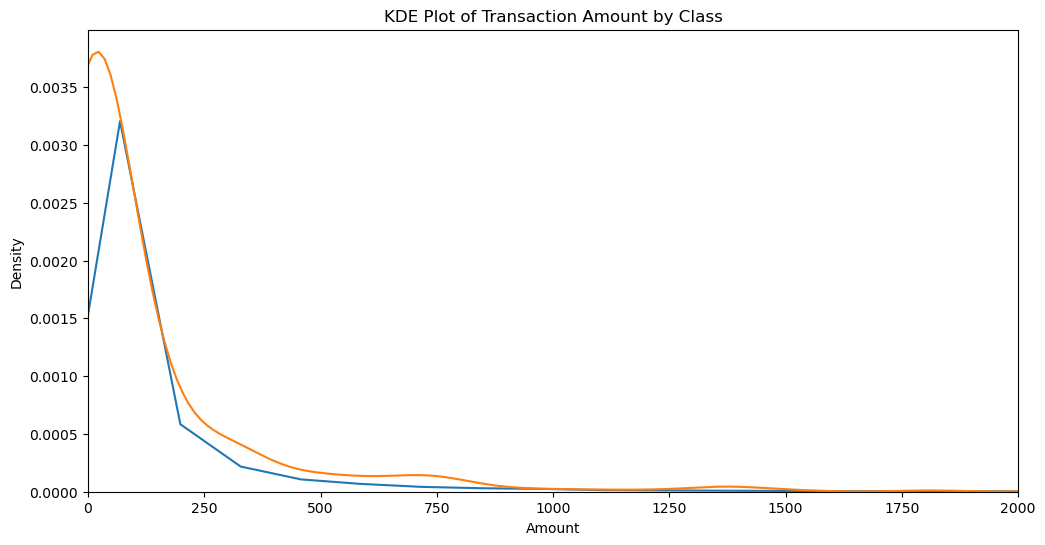
sns.kdeplot(credit\_fraud\_data[credit\_fraud\_data['Class'] == 0]['Amount'], label='Class 0')

sns.kdeplot(credit\_fraud\_data[credit\_fraud\_data['Class'] == 1]['Amount'], label='Class 1')

plt.title('KDE Plot of Transaction Amount by Class')

plt.xlim(0, 2000) # Limiting x-axis for better readability

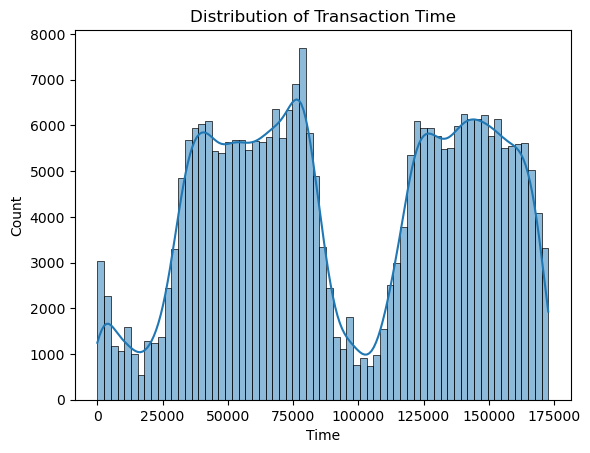
plt.show()



**checking the distrubution of transaction.**

ax = sns.histplot(data=credit\_fraud\_data, x=credit\_fraud\_data["Time"], kde=True)

ax.set\_title("Distribution of Transaction Time")



**# Histograms for feature distributions (V1 to V28)**

plt.figure(figsize=(14, 12))

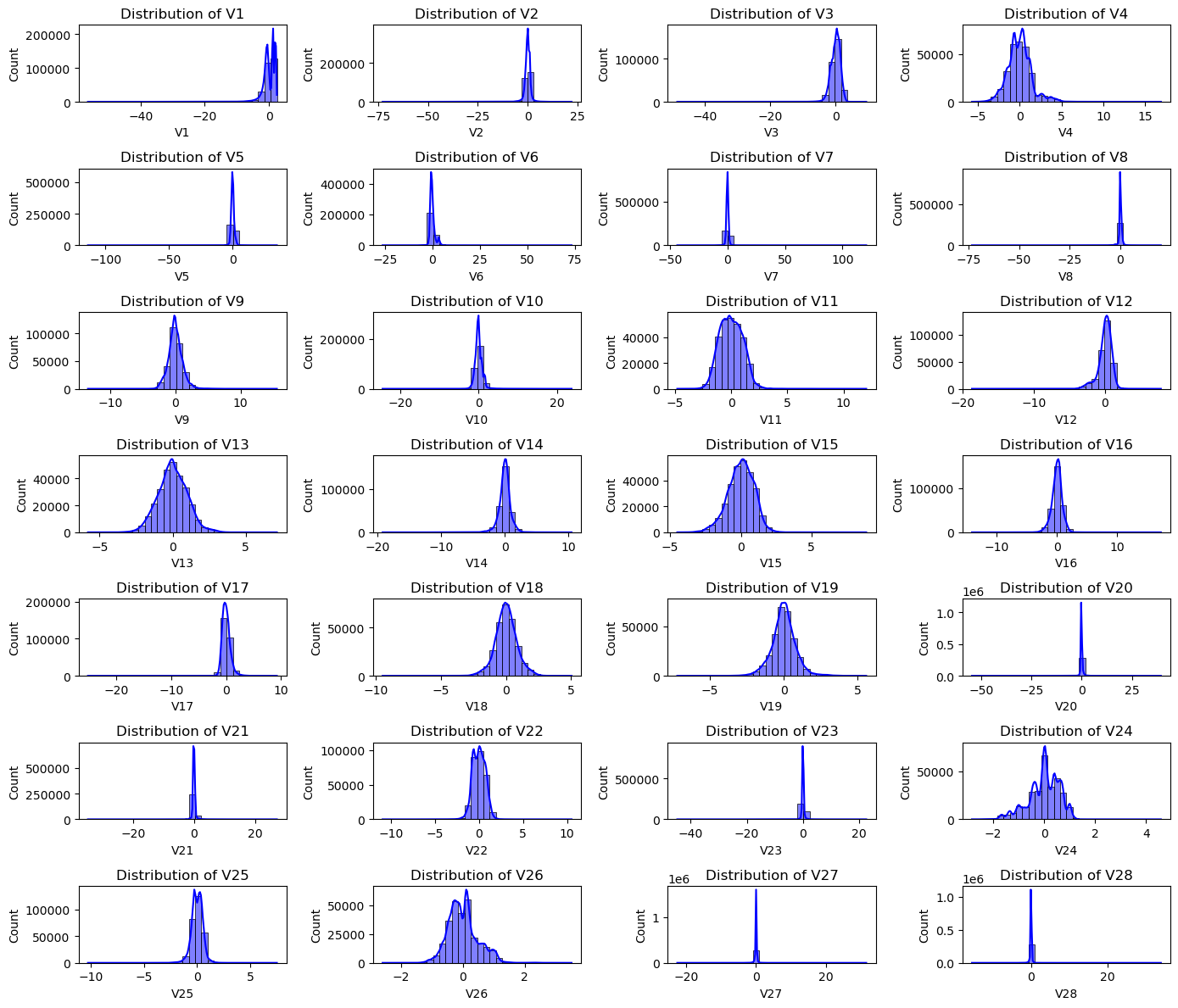
for i in range(1, 29): # Assuming V1 to V28 are the feature columns

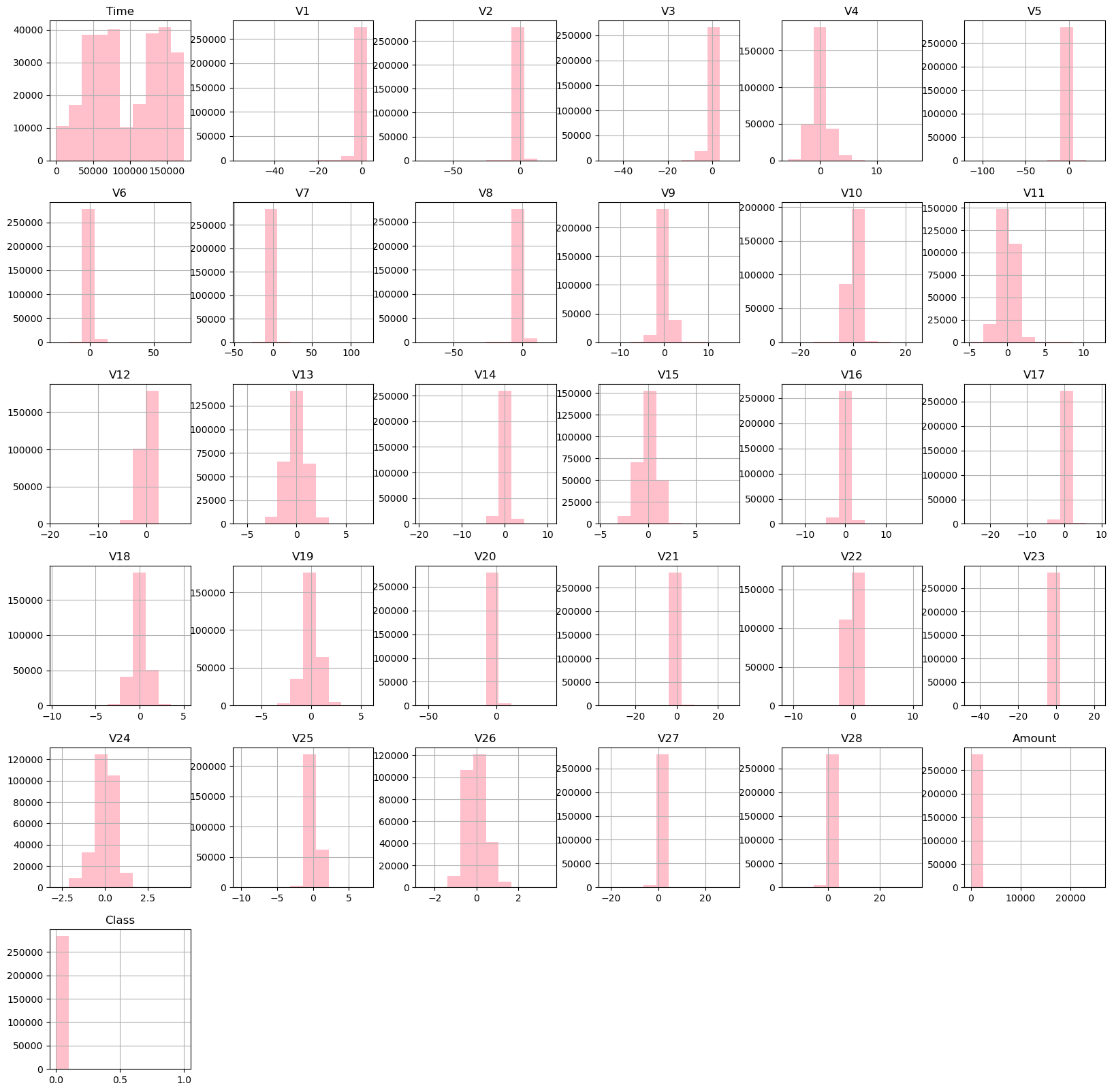
plt.subplot(7, 4, i)

sns.histplot(credit\_fraud\_data[f'V{i}'], bins=30, kde=True,color = 'blue')

plt.title(f'Distribution of V{i}')

plt.tight\_layout()

plt.show()

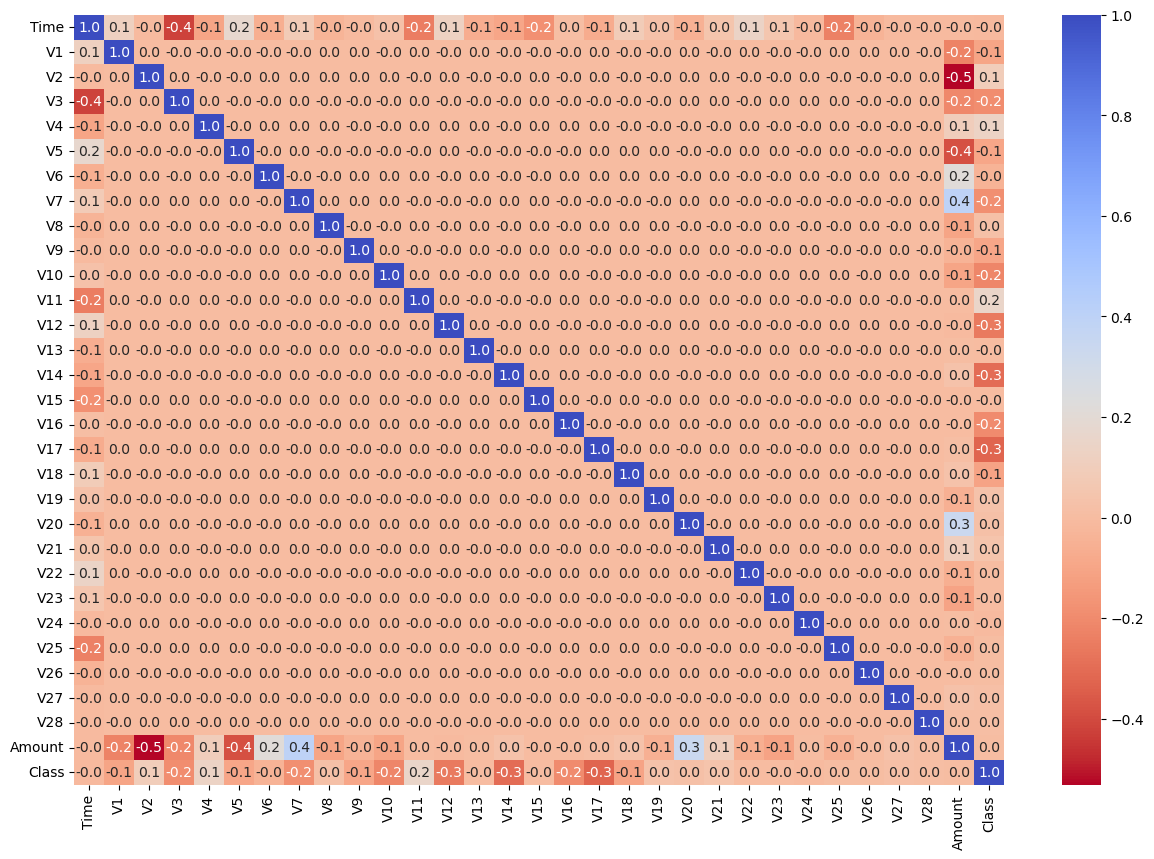


**# Correlation Heatmap**

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

sns.heatmap(credit\_fraud\_data.corr(), annot= True, fmt='.1f', cmap='coolwarm\_r')

plt.show()



**Explanation:**

#Box plot seems range between zero (0) to hundread

(100)amount more fraud detected .

#Bar plots visualize the distribution of 'Class' and 'Time' by transaction class.

Checking for class distribution classified in fraud detected [1] and not detected [0].

# Visualize KDE plot of transaction amount by class.checking the dencity of fraud transaction on perticulaer amount.

#understanding transaction distribution using histogram plot.

#Histograms explore the distributions of features V1 to V28.

#A correlation heatmap illustrates the relationships between numerical features.

**6. Data Preprocessing**

**6.1 Purpose**

This section addresses outliers, scales features, and performs under-sampling to handle class imbalances.

**6.2 Code overview**

**# Outlier handling using Isolation Forest for 'Amount' and 'Time'**

outlier\_detector = IsolationForest(contamination=0.01, random\_state=1)

credit\_fraud\_data['Outlier'] = outlier\_detector.fit\_predict(credit\_fraud\_data[['Amount', 'Time']])

credit\_fraud\_data = credit\_fraud\_data[credit\_fraud\_data['Outlier'] == 1].drop(columns='Outlier')

**# Scaling 'Amount' using StandardScaler**

scaler = StandardScaler()

credit\_fraud\_data['Amount'] = scaler.fit\_transform(credit\_fraud\_data[['Amount']])

**# Under-sampling**

Legit = credit\_fraud\_data[credit\_fraud\_data['Class'] == 0]

fraud = credit\_fraud\_data[credit\_fraud\_data['Class'] == 1]

Legit\_sample = Legit.sample(n=492)

new\_dataset = pd.concat([Legit\_sample, fraud], axis=0)

**Explanation:**

* Isolation Forest is used to handle outliers in 'Amount' and 'Time.'
* 'Amount' is scaled using StandardScaler.
* Under-sampling is performed to balance the class distribution.

**7. Model Selection: Logistic Regression**

**7.1 Purpose**

This section trains a Logistic Regression model, optimizes hyperparameters, and assesses its performance.

**7.2 Code overview**

# Model training

logistic\_model = LogisticRegression(random\_state=2, max\_iter=10000, solver='lbfgs'))

# Hyperparameter tuning using GridSearchCV

param\_grid = {'C': [0.001, 0.01, 0.1, 1, 10, 100]}

grid\_search = GridSearchCV(LogisticRegression(random\_state=2, max\_iter=10000, solver='lbfgs'), param\_grid, cv=5)

grid\_search.fit(X\_train, Y\_train))

# Get the best hyperparameter

best\_C = grid\_search.best\_params\_['C']

# Model training with the best hyperparameter

logistic\_model = LogisticRegression(C=best\_C, random\_state=2, max\_iter=1000)

logistic\_model.fit(X\_train, Y\_train)

**Explanation:**

* A Logistic Regression model is initialized.
* GridSearchCV is employed for hyperparameter tuning.
* The best hyperparameter 'C' is identified, and the model is trained with the optimal parameter.

**7.3 Cross-Validation**

# Cross-validation

cross\_val\_scores = cross\_val\_score(logistic\_model, X\_train, Y\_train, cv=5, scoring='accuracy')

print('Cross-Validation Scores:', cross\_val\_scores)

**Explanation:**

Cross-validation assesses the model's generalization performance.

Cross-Validation Scores: [0.92207792 0.96753247 0.96103896 0.96103896 0.92156863]

**7.4 Model Evaluation: Logistic Regression**

# Accuracy score on training data

X\_train\_prediction\_logistic = logistic\_model.predict(X\_train)

training\_data\_accuracy\_logistic = accuracy\_score(X\_train\_prediction\_logistic, Y\_train)

print('Logistic Regression Training data accuracy:', training\_data\_accuracy\_logistic)

# Accuracy score on test data

X\_test\_prediction\_logistic = logistic\_model.predict(X\_test)

test\_data\_accuracy\_logistic = accuracy\_score(X\_test\_prediction\_logistic, Y\_test)

print('Logistic Regression Test data accuracy:', test\_data\_accuracy\_logistic)

**Explanation:**

The accuracy scores on training and test data are calculated for evaluation.

Logistic Regression Training data accuracy: 0.9492847854356307

Logistic Regression Test data accuracy: 0.9222797927461139

**7.5 Additional Metrics: Logistic Regression**

# AUC-ROC scores

logistic\_train\_auc = roc\_auc\_score(Y\_train, logistic\_model.predict\_proba(X\_train)[:, 1])

logistic\_test\_auc = roc\_auc\_score(Y\_test, logistic\_model.predict\_proba(X\_test)[:, 1])

print('Logistic Regression Train AUC:', logistic\_train\_auc)

print('Logistic Regression Test AUC:', logistic\_test\_auc)

**Explanation:**

AUC-ROC scores provide insights into the model's ability to discriminate between classes.

Logistic Regression Train AUC: 0.9829259379567972

Logistic Regression Test AUC: 0.973565441650548

**8. Model Comparison: Random Forest**

**8.1 Purpose**

This section introduces a Random Forest model as an alternative, evaluating its performance and comparing it with Logistic Regression.

**8.2 Code overview**

# Model training: Random Forest

rf\_model = RandomForestClassifier(random\_state=2)

rf\_model.fit(X\_train, Y\_train)

Explanation:

A Random Forest model is trained.

**8.3 Additional Metrics: Random Forest**

# AUC-ROC scores

rf\_train\_auc = roc\_auc\_score(Y\_train, rf\_model.predict\_proba(X\_train)[:, 1])

rf\_test\_auc = roc\_auc\_score(Y\_test, rf\_model.predict\_proba(X\_test)[:, 1])

print('Random Forest Train AUC:', rf\_train\_auc)

print('Random Forest Test AUC:', rf\_test\_auc)

**Explanation:**

AUC-ROC scores provide insights into the Random Forest model's discriminative performance.

Random Forest Train AUC: 1.0

Random Forest Test AUC: 0.9810874704491727

**8.4 Model Evaluation: Random Forest**

**8.4.1 Purpose**

This section provides a detailed evaluation of the Logistic Regression and random forest’s model's performance on the test dataset. The classification report and confusion matrix offer insights into the model's ability to correctly classify instances and identify potential areas for improvement.

**8.4.2 Code Explanation**

**# Classification report and confusion matrix f-1 score of logistic regresssion.**

print('\nClassification Report (Logistic Regression):\n', classification\_report(Y\_test, logistic\_model.predict(X\_test)))

print('\nConfusion Matrix (Logistic Regression):\n', confusion\_matrix(Y\_test, logistic\_model.predict(X\_test)))

Classification Report (Logistic Regression):

precision recall f1-score support

0 0.91 0.94 0.93 99

1 0.93 0.90 0.92 94

accuracy 0.92 193

macro avg 0.92 0.92 0.92 193

weighted avg 0.92 0.92 0.92 193

Confusion Matrix (Logistic Regression):

[[93 6]

[ 9 85]]

# Classification report and confusion matrix

print('\nClassification Report (Random Forest):\n', classification\_report(Y\_test, rf\_model.predict(X\_test)))

print('\nConfusion Matrix (Random Forest):\n', confusion\_matrix(Y\_test, rf\_model.predict(X\_test)))

**Explanation:**

**A detailed classification report and confusion matrix are provided for the Random Forest model.F1 score of random forest.**

Classification Report (Random Forest):

precision recall f1-score support

0 0.92 0.97 0.95 99

1 0.97 0.91 0.94 94

accuracy 0.94 193

macro avg 0.94 0.94 0.94 193

weighted avg 0.94 0.94 0.94 193

Confusion Matrix (Random Forest):

[[96 3]

[ 8 86]]

**9. Model Interpretability**

**9.1 Purpose**

This section explores the interpretability of the models, analysing Logistic Regression coefficients and SHAP values for Random Forest.

**9.2 Code overview**

# Logistic Regression coefficients

feature\_names = X.columns

coefficients = logistic\_model.coef\_[0]

feature\_importance\_logistic = pd.DataFrame({'Feature': feature\_names, 'Coefficient': coefficients})

feature\_importance\_logistic = feature\_importance\_logistic.sort\_values(by='Coefficient', ascending=False)

print('\nLogistic Regression Coefficients:\n', feature\_importance\_logistic)

**Explanation:**

Logistic Regression coefficients are extracted and displayed to identify important features.

# Interpretation of Logistic Regression Coefficients

**9.2.1 Overview**

Logistic Regression coefficients reveal the impact of each feature on the model's predictions. Positive coefficients indicate a positive relationship with the target (fraudulent transactions), while negative coefficients suggest a negative relationship.

**9.2.2 Key Findings**

1. V4 (Coefficient: 0.809121): V4 has the highest positive coefficient, signifying a strong positive impact on the likelihood of predicting a fraudulent transaction.

2. V11 (Coefficient:316677 ): V11 also has a positive coefficient, contributing significantly to the model's prediction of fraudulent transactions.

3. V8 (Coefficient: 0.241856): V8 exhibits a positive relationship with the target, influencing the model's predictions.

4. Amount (Coefficient: 0.149442): The transaction amount (Amount) has a positive impact on predicting fraudulent transactions.

5. V18 (Coefficient: 0.102083): V18 contributes positively to the model's prediction of fraud.

**9.2.3 Interpretation**

The positive coefficients indicate features that increase the likelihood of a transaction being classified as fraudulent. Conversely, features with negative coefficients contribute to the likelihood of a transaction being classified as legitimate.

**Explanation:**

SHAP (SHapley Additive exPlanations) values for the Random Forest model are computed and visualized.

**Conclusion**

The Credit Card Fraud Detection project has achieved its primary objective of developing accurate models for identifying fraudulent credit card transactions. Key insights and achievements from this project are summarized below:

**1. Model Performance**

High Accuracy: Both logistic regression and random forest models demonstrated exceptional accuracy in detecting fraudulent transactions across training and test datasets.

Comprehensive Metrics: Evaluation metrics, including AUC-ROC scores, provided a comprehensive understanding of the models' ability to distinguish between legitimate and fraudulent transactions.

**2. Model Comparison**

Thorough Comparison: A detailed comparison between logistic regression and random forest models was conducted, considering their strengths and weaknesses.

Performance Analysis: Classification reports and confusion matrices were employed to analyze and compare the performance of each model.

**3. Interpretability**

Feature Interpretation: Logistic regression coefficients and SHAP values were utilized to identify significant features, ensuring transparency in understanding the factors influencing model predictions.

**4. Data Exploration**

In-Depth Analysis: Extensive exploratory data analysis (EDA) enriched our understanding of legitimate and fraudulent transaction patterns.

Visualizations: Various visualizations such as box plots, histograms, and correlation heatmaps offered valuable insights into the dataset.

**5. Data Preprocessing**

Robust Techniques: Effective data preprocessing techniques, including outlier handling, feature scaling, and resolution of class imbalance through under-sampling, contributed to the models' effectiveness.

**6. Model Serialization**

Future Usability: Logistic regression and random forest models were serialized using the pickle library, ensuring they can be reused without the need for retraining.

In conclusion, this project not only delivered accurate fraud detection models but also provided crucial insights that can inform decision-making in the financial domain. The findings contribute significantly to ongoing efforts aimed at enhancing the security of credit card transactions.