Machine Learning Project Based Learning (PBL) Report on

## ONLINE PAYMENT FRAUD DETECTION IN MACHINE LEARNING

Submitted in partial fulfilment of the Requirements for the award of the degree of **BACHELOR OF TECHNOLOGY**

in

##### CSE (Cyber Security)

***Submitted by***

##### Thakur Tejaehwar Singh [21R11A6258] Yama Shiva Prasad [21R11A6263]

**Sahith Chandra Poreddy [21R11A6248]**

**Kasipaka Koushik [22R15A6204]**

***Under the esteemed guidance of***

##### Mr. Vikram Sindhu

Assoc. Professor, CSE(Cyber Security) Department Geethanjali College of Engineering and Technology



Geethanjali College of Engineering and Technology

***Department of CSE (Cyber Security)***

#### (UGC AUTONOMOUS INSTITUTION)

**Accredited by NAAC with ‘A+’ Grade & NBA, Approved by AICTE and Affiliated to JNTUH Cheeryal (V), Keesara (M), Medchal (Dist), Telangana – 501 301.**

#### JUNE - 2024



Geethanjali College of Engineering and Technology

***Department of CSE (Cyber Security)***

#### (UGC AUTONOMOUS INSTITUTION)

**Accredited by NAAC with ‘A+’ Grade & NBA, Approved by AICTE and Affiliated to JNTUH Cheeryal (V), Keesara (M), Medchal (Dist), Telangana – 501 301.**

**JUNE – 2024**

**DEPARTMENT OF CSE (Cyber Security)**

## CERTIFICATE

This is to certify that the Machine Learning Project Based Learning (PBL) Report entitled **“Online Payment Fraud Detection”** is a bonafide work done and submitted by **Thakur Tejaeshwar Singh (21R11A6258) , Yama Shiva Prasad (21R11A6263) and Sahith Chandra Poreddy (21R11A6248), Kasipaka Koushik (22R15A6204)** during the academic year 2023 – 2024, in partial fulfilment of requirement for the award of Bachelor of Technology degree in **“CSE Cyber Security)”** from Geethanjali College of Engineering and Technology (Accredited by NAAC with ‘A+’ Grade & NBA, Approved by AICTE and Affiliated to JNTUH), is a bonafide record of work carried out by them under guidance and supervision.

Certified further that to my best of the knowledge, the work in this project has not been submitted to any other institution for the award of any degree or diploma.

#### FACULTY GUIDE HEAD OF THE DEPARTMENT

##### Mr. Vikram Sindhu Dr. G. Kalyani

Associate Professor Professor & HOD

CSE(Cyber Security) Department CSE(Cyber Security) Department

# DECLARATION

We hereby declare that the project report entitled **“Online Payment Fraud Detection”** is an original work done and submitted to CSE(AI&ML) Department, from Geethanjali College of Engineering and Technology (Accredited by NAAC with ‘A+’ Grade & NBA, Approved by AICTE and Affiliated to JNTUH), in partial fulfilment of the requirement for the award of Bachelor of Technology in **“CSE (Cyber Security)”** and it is a record of bonafide project work carried out by us under the guidance of **Mr. Vikram Sindhu, Associate Professor, Department of CSE(Cyber Security)**.

We further declare that the work reported in this project has not been submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other Institute or University.

Signature of the Student

Thakur Tejaeshwar Singh (21R11A6258)

Signature of the Student

Yama Shiva Prasad (21R11A6263)

Signature of the Student Poreddy Sahith Chandra

(21R11A6248)

Signature of the Student Kasipaka Koushik

(22R15A6204)

# ACKNOWLEDGEMENT

This satisfaction of completing this project would be incomplete without mentioning our gratitude towards all the people who have supported us. Constant guidance and encouragement have been instrumental in the completion of this project.

First and foremost, we thank the chairman, Principal, Vice Principal for availing infrastructural facilities to complete the project in time.

We offer our sincere gratitude to our faculty guide **Mr. Vikram Sindhu,** Associate Professor, CSE(Cyber Security) Department, from Geethanjali College of Engineering and Technology (Accredited by NAAC with ‘A+’ Grade & NBA, Approved by AICTE and Affiliated to JNTUH), for his immense support, timely co-operation and valuable advice throughout the course of our project work.

We would like to thank the Head of Department, **Dr. G Kalyani,** for his meticulous care and co-operation throughout the project work.

We are thankful to all the project Coordinators for their supportive guidance and for having provided the necessary help for carrying forward this project without any obstacle and hindrances.

## ABSTRACT

As online transactions become more prevalent, the risk of fraudulent activities also increases, posing significant security threats. The increased usage of online payments is leading to a rise in fraud. Fraud detection is an important component of online payment systems since it serves to protect both customers and merchants from financial damages. This project aims to address online payment fraud detection using advanced machine learning techniques. By analyzing transaction data—such as transaction type, amount, sender and receiver details, and account balances. Our approach involves training the model on a diverse dataset to recognize patterns and anomalies indicative of fraud. We will explore various machine learning algorithms. The performance of these algorithms will be evaluated using metrics like accuracy, precision, recall, and F1-score to identify the most effective model. The ultimate goal is to enhance the security of online payment systems, fostering trust and confidence among users. By effectively detecting and mitigating fraudulent transactions, we aim to protect individual users and bolster the integrity of digital financial systems. This will support the continued growth and adoption of online payment methods, ensuring safer digital transactions for all stakeholders.

**Keywords:** Machine learning Techniques, fraudulent transactions, Safer digital Transactions, Security enhancement.

### TABLE OF FIGURES

|  |  |  |
| --- | --- | --- |
| S. No | Name of Figure | Page Number |
| 1. | Online Payment | 1 |
| 2. | Random forest Classifier | 8 |
| 3. | Support Vector Machine | 9 |
| 4. | AdaBoost Classifier | 9 |
| 5. | Training and Testing | 14 |
| 6. | Visualizations | 17-18 |
| 7. | Outputs | 19-20 |

# TABLE OF CONTENTS

[CERTIFICATE i](#_bookmark0)

[DECLARATION ii](#_bookmark1)

[ACKNOWLEDGEMENT iii](#_bookmark2)

[ABSTRACT iv](#_bookmark3)

[TABLE OF FIGURES v](#_bookmark4)

1. INTRODUCTION 1
   1. [Online Payments 1](#_TOC_250005)
   2. [Advantages of Online Payments 1](#_TOC_250004)
2. AIM AND OBJECTIVE 3
3. BACKGROUND 4
4. LITERATURE REVIEW 5
5. SOFTWARE REQUIREMENT SPECIFICATION 6
   1. Functional Requirements 6
   2. Non – Functional Requirements 6
   3. System Requirements 6
   4. Performance Requirements 7
   5. Documentation Requirements 7
6. MODELS APPLIED 8
   1. [Random Forest Classifier 8](#_TOC_250003)
   2. [Support Vector Machine 8](#_TOC_250002)
   3. AdaBoost Classifier 9
7. DATASETS AND PREPROCESSING 10
   1. [Datasets 10](#_TOC_250001)
   2. [Pre-processing 10](#_TOC_250000)
8. IMPLEMENTATION 12
9. TRAINING AND TESTING 13
   1. Testing Method 13
   2. Training Method 13
10. SOURCE CODE 15-16
11. **VISUALLIZATIONS 17-18**
12. **OUTPUT 19-20**
13. **CONCLUSION 21**
14. **FUTURE SCOPE 22**
15. **REFERENCES 23**

#### ONLINE PAYMENTS

## INTRODUCTION

In recent years, online payments have revolutionized the way we conduct financial transactions, offering convenience, speed, and accessibility like never before. With the rise of e-commerce platforms, mobile banking apps, and digital wallets, consumers now have the flexibility to make purchases, transfer funds, and pay bills from the comfort of their own homes or on the go. This shift towards digital payment methods has not only transformed the retail landscape but has also reshaped the entire financial ecosystem.

Online payments encompass a wide range of transactions, including online shopping, bill payments, peer-to-peer transfers, and subscription services. These transactions are facilitated through various channels, such as credit and debit cards, bank transfers, mobile payment apps, and digital currencies like Bitcoin. The seamless integration of technology and finance has democratized access to financial services, empowering individuals and businesses to participate in the global economy regardless of geographical barriers.



**Fig 1.1 Online Payment**

#### ADVANTAGES OF ONLINE PAYMENTS

Online payments offer numerous advantages for both consumers and businesses, transforming the way transactions are conducted in today's digital world. Here are some key benefits:

1. Convenience:

One of the most significant advantages of online payments is the convenience they provide. Consumers can make payments from anywhere and at any time, eliminating the need to visit physical stores or banks. This 24/7 accessibility simplifies the purchasing process, making it easier for customers to buy products and services on the go.

1. Speed and Efficiency

Online payments are typically processed much faster than traditional payment methods such as checks or bank transfers. Transactions are completed in real-time or within a few hours, allowing businesses to receive funds quicker and customers to access goods and services without delay.

1. Enhanced Security

Modern online payment systems incorporate advanced security measures such as encryption, tokenization, and multi-factor authentication. These technologies help protect sensitive financial information from fraud and unauthorized access, providing a safer transaction environment for both parties.

1. Cost-Effectiveness

For businesses, online payments can be more cost-effective compared to traditional methods. They reduce the need for physical infrastructure, lower transaction fees compared to bank transfers, and minimize the costs associated with handling cash. Additionally, automation of payment processing reduces administrative expenses.

1. Reduced Risk of Theft

With online payments, the risk of physical theft is significantly reduced. There is no need to handle large amounts of cash, which can be vulnerable to robbery or loss. Digital transactions also provide a secure trail that can be traced and audited if necessary.

## AIM AND OBJECTIVE

The aim and objectives of online payment fraud detection is to safeguard financial transactions from fraudulent activities, thereby protecting both consumers and businesses. This involves identifying and preventing unauthorized transactions in real-time to maintain the integrity and trust of digital payment systems. Here are some aims and objectives:

1. Identify Fraudulent Transactions: Develop and implement systems to detect and flag potentially fraudulent transactions by analyzing patterns and anomalies in transaction data.
2. Minimize Financial Loss: Reduce the financial impact of fraud on businesses and consumers by swiftly identifying and preventing fraudulent activities.
3. Enhance Security Measures: Continuously improve the security protocols and technologies used to protect online payment systems from evolving fraud tactics.
4. Ensure Compliance: Adhere to regulatory requirements and industry standards for fraud prevention and data protection to ensure legal and ethical compliance.
5. Improve User Trust: Build and maintain consumer confidence in online payment systems by ensuring their transactions are secure and protected from fraud.
6. Facilitate Rapid Response: Establish protocols for quick response and resolution when fraudulent activity is detected, minimizing the time and effort required to address fraud incidents.
7. Collaborate with Stakeholders: Work with financial institutions, regulatory bodies, and other stakeholders to share information and best practices for combating online payment fraud.

By focusing on these objectives, online payment fraud detection systems aim to create a secure environment for digital transactions, fostering trust and reliability in the growing landscape of online commerce.

## BACKGROUND

The study of online payment fraud detection has evolved significantly over the past few decades. Initially, fraud detection methods were basic and largely manual, focusing on simple rules and pattern recognition to identify suspicious transactions. Early fraud detection efforts were hampered by limited technology and data availability, making it challenging to effectively combat fraudulent activities.

As digital transactions became more prevalent, the need for more sophisticated fraud detection mechanisms grew. The 21st century saw significant advancements in technology, including the development of machine learning, artificial intelligence (AI), and big data analytics. The implementation of multi-factor authentication (MFA), encryption, and tokenization further enhanced the security of online payment systems. These technologies help protect sensitive financial information and reduce the risk of unauthorized access and fraud.

In recent years, the scope of online payment fraud detection has expanded to include behavioural analytics, geolocation tracking, and device fingerprinting. These techniques allow for a more comprehensive analysis of user behaviour and transaction context, improving the ability to detect and prevent fraud.

Today, online payment fraud detection is a critical component of financial security, employing advanced algorithms and collaborative efforts among financial institutions to stay ahead of evolving fraud tactics. Ongoing research and development in this field aim to enhance the accuracy and effectiveness of fraud detection, ultimately protecting consumers and businesses and maintaining trust in digital financial transactions.

## LITERATURE REVIEW

* Abdulwahab Ali Almazori [1] et al. proposed a methodology for online payment fraud detection using machine learning techniques. They applied Synthetic Minority Over-sampling Technique (SMOTE) algorithm to address class imbalance and used the Ensemble Auto Encoder with ResNet (EARN) model for feature extraction, subsequently developed a model RXT-J achieving good results with this approach.
* Bhukya Keerthi Bai [2] et al. developed a web-based application for online payment fraud detection using machine learning techniques. They have used the random forest classifier for classification which gave them the good results.
* Mr. Ganesh Pawar [3] et al. applied various machine learning techniques for online payment fraud detection system. The algorithms that are used are KNN, XGBoost and Random Forest. Their study shows that XGBoost gives good result when compare to other algorithms that are used in their work on the dataset they have chosen.
* Naga Babu Pachhala [4] et al. They used algorithms like SVM and Random Forest for online payment fraud detection. Their project concludes that random forest algorithm gave the best results than other algorithms used

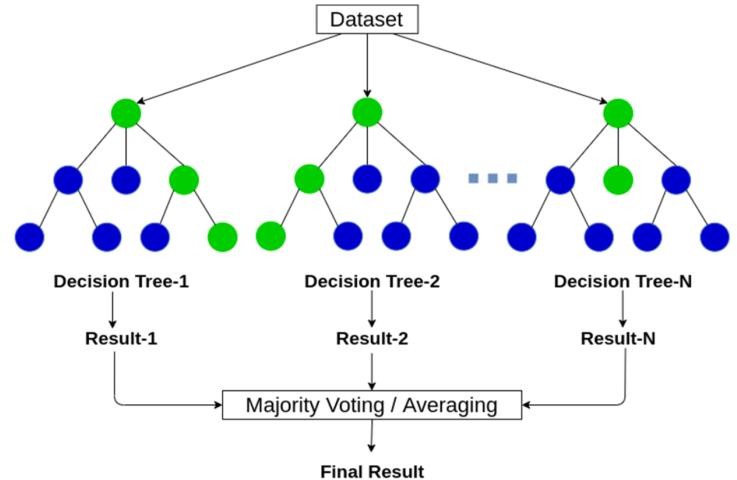
## SOFTWARE REQUIREMENTS SPECIFICATION

* 1. Functional Requirements:
     + Real-Time Detection: The system should be able to detect and flag potentially fraudulent transactions in real-time.
     + High Volume Handling: The system should be capable of processing and analyzing large volumes of transactions simultaneously.
     + Model Updating: The system should automatically update its fraud detection model based on new data to adapt to emerging fraud patterns.
     + Feedback Mechanism: The system should allow feedback on false positives and false negatives to improve future detection accuracy.
     + Integration: The system should seamlessly integrate with existing payment processing systems and platforms.
  2. Non-Functional Requirements:
     + Accuracy: The system should have a high accuracy rate in detecting fraudulent transactions.
     + Low False Positive Rate: The system should minimize the number of legitimate transactions incorrectly flagged as fraudulent.
     + Efficiency: The system should operate quickly and efficiently, with minimal impact on overall system performance.
     + Security: The system should ensure the security and confidentiality of transaction data, preventing unauthorized access.
     + User-Friendliness: The system should be easy to install, configure, and use by IT administrators and end-users.
  3. System Requirements:
     + Compatibility: The system should be compatible with various operating systems, including Windows, Mac, and Linux.
     + Resource Efficiency: The system should require minimal hardware resources to operate effectively.
     + Scalability: The system should be scalable to handle increasing volumes of transactions as the business grows.
  4. Performance Requirements:
     + Speed: The system should be able to detect and flag fraudulent transactions within a few seconds.
     + High Volume Handling: The system should maintain performance and not cause slowdowns or crashes even under high transaction volumes.
     + Adaptability: The system should adapt to changes in fraud patterns and continuously improve its detection accuracy.
  5. Documentation Requirements:
     + Comprehensive Documentation: The system should come with detailed documentation on installation, configuration, and use.
     + Algorithm Documentation: The system should provide clear documentation on the fraud detection algorithms used, including information about the datasets used for training.

## MODELS APPLIED

##### Random Forest Classifier

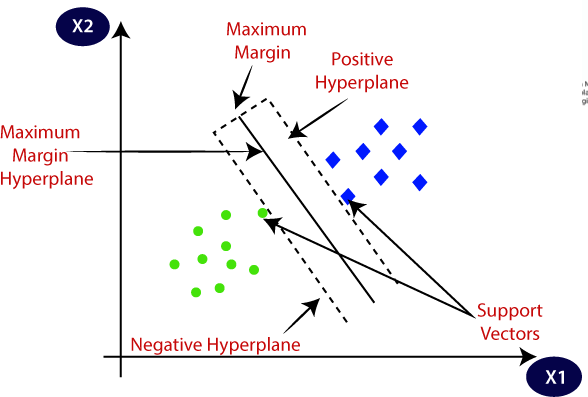
The Random Forest classifier is an ensemble learning method that excels in both classification and regression tasks. It leverages the collective power of multiple decision trees to produce robust and accurate predictions. The essence of this technique lies in creating a 'forest' of decision trees, each trained on a different subset of the data and considering different subsets of features. This process introduces randomness, which helps in reducing overfitting and improving the model’s generalization ability.



##### Fig 6.1 Random Forest Classifier

##### Support Vector Machine

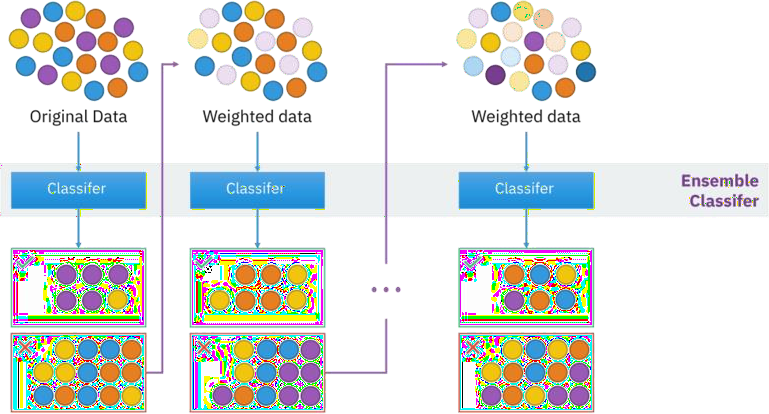
Support Vector Machine (SVM) is a robust supervised learning algorithm used for classification and regression tasks. It works by finding the optimal hyperplane that best separates the data points of different classes. In two dimensions, this hyperplane is a line, while in higher dimensions, it becomes a plane or hyperplane. The key to SVM is maximizing the margin, which is the distance between the hyperplane and the nearest data points from each class, known as support vectors. By focusing on these support vectors, SVM achieves a robust classification that can generalize well to unseen data.



**Fig 6.2 Support Vector Machine**

* 1. AdaBoost classifier

The AdaBoost (Adaptive Boosting) classifier is an ensemble learning method designed to enhance the performance of weak classifiers by combining them to form a stronger overall model. AdaBoost starts by assigning equal weights to all training samples. A weak classifier, such as a decision tree stump, is then trained on this weighted dataset. The performance of this classifier is evaluated, and its error rate is calculated. The key innovation in AdaBoost is its iterative process of updating the weights of the training samples: samples that are misclassified by the weak classifier receive increased weights, making them more significant in the subsequent round of training.



**Fig 6.3 AdaBoost Classifier**

## DATASETS AND PREPROCESSING

Datasets and pre-processing are critical components of Online Payment Fraud Detection. Here is an overview of each:

##### Datasets

Datasets for online payment fraud detection contain labeled examples of transactions, where each transaction is labeled as either fraudulent or legitimate. These datasets typically include various features that provide information about each transaction. It contains 10049 rows and 11 columns.

##### Preprocessing

Before training a machine learning model on a dataset, it's important to pre-process the data. This typically involves the following steps:6

##### Handling Missing Values:

* + - * Identification: The dataset is scanned for missing values using methods like. isna() or. isnull().
      * Imputation: Missing values are addressed through techniques such as mean, median, mode imputation, or using more advanced methods like interpolation.
      * missing values are replaced with appropriate values using methods like. fillna ().

##### Data Encoding:

* + - * Categorical variables are encoded into numerical format as machine learning models typically require numerical input.
      * Common encoding techniques include one-hot encoding for nominal categorical variables and label encoding for ordinal categorical variables.
      * categorical variables are encoded using pd.get dummies().

##### Feature Scaling:

* + - * Numerical features are often scaled to a standard range to prevent features with larger scales from dominating during model training.
      * Standardization (scaling to mean 0 and standard deviation 1) or Min- Max scaling (scaling to a range between 0 and 1) are common techniques.
      * In the provided code, numerical features are scaled using StandardScaler() from sklearn preprocessing.

##### Outlier Detection and Handling:

* + - * Outliers, if present, can adversely affect model performance. Therefore, it's crucial to identify and address outliers appropriately.
      * Techniques like visualization (box plots, scatter plots) and statistical methods (Z- score, IQR) can be employed to detect outliers.
      * outlier detection is performed using visualization techniques like box plots.

##### Feature Selection:

* + - * Feature selection involves choosing the most relevant features that contribute significantly to the target variable.
      * Techniques such as univariate feature selection, recursive feature elimination, or feature importance from tree-based models can be employed.
      * While not explicitly shown, feature selection is often performed before or during model training to improve model efficiency and interpretability.

## IMPLEMENTATION

##### Step 1: Data Preparation

The first step is to prepare the data. This involves gathering a labeled dataset of online payment transactions, where each transaction is labeled as fraudulent or legitimate. Pre-process the data, which may include handling missing values, encoding categorical variables, and scaling numerical features. Split the dataset into training and testing sets.

##### Step 2: Model Selection

The next step is to select a machine learning model to use for Online Payment Fraud Detection. Commonly used models include Random Forests, Support Vector Machine (SVM), KNN, Logistic Regression. Consider factors such as the dataset size, complexity of fraud patterns, interpretability of the model, and computational resources available.

##### Step 3: Model Training

Once a model has been selected, it needs to be trained on the pre-processed data.This involves splitting the data into training and testing sets and using the training set to fit the model to the data. The performance of the model can then be evaluated using metrics such as accuracy, precision, recall, and F1 score.

##### Step 4: Model Tuning

After training the model, it may be necessary to tune the model's hyperparameters to improve its performance. Perform grid search or random search over a range of hyperparameters to find the optimal combination. Validate the tuned model on the testing set to ensure generalization performance.

##### Step 5: Model Deployment

Deploy the trained and tuned model into a production environment for real-time fraud detection. Integrate the model with the online payment system to automatically classify incoming transactions as fraudulent or legitimate.

Implementing online payment fraud detection using machine learning can help financial institutions and online businesses to detect and prevent fraudulent transactions effectively.

## TRAINING AND TESTING

#### TRAINING

* + 1. Dataset Partitioning: The dataset is divided into two subsets: the training set and the testing set. The training set typically comprises around 80% of the data, while the testing set contains the remaining 20%. This partitioning ensures that the models are trained on a sufficient amount of data while still having unseen data for evaluation.
    2. Model Selection: Various machine learning models, such as Decision Tree Classifier, Random Forest Classifier, Logistic Regression, and Support Vector Machines (SVM), are chosen based on the specific requirements and characteristics of the dataset. Each model is selected for its ability to capture complex patterns and relationships within the data.
    3. Model Training: The selected models are trained on the training set using the fit() method provided by machine learning libraries. During training, the models learn from the input features and adjust their internal parameters to minimize the difference between their predictions and the actual targetvalues.This process involves iterative optimization algorithms, such as gradient descent, to update the model's parameters based on the error between predicted and actual values.
    4. Importance of Training: During training, models learn to identify patterns and relationships within the data that are indicative of fraudulent behaviour.

#### TESTING

* + 1. Evaluation Data Preparation: The testing set, typically comprising around 20% of the dataset, is separated from the training set. This ensures that the models are evaluated on unseen data, simulating real-world scenarios.
    2. Model Prediction: Trained models are used to predict the target variable (presence or absence of insurance fraud) based on the features of the testing set. This is typically done using the predict() method provided by machine learning libraries.
    3. Performance Evaluation: Predicted values are compared with the actual target values in the testing set to assess the models' performance. Various metrics such as accuracy, precision, recall, F1-score, and confusion matrix are computed to evaluate the models' effectiveness. These metrics provide insights into the models' ability to correctly classify instances of insurance fraud and their overall performance.
    4. Model Selection:Based on the evaluation results, the most effective model(s) are identified for deployment in real-world scenarios. Factors such as accuracy, precision, recall, and the specific requirements of the insurance fraud detection task are considered when selecting the final model(s).

Importance of Testing: Testing on unseen data allows us to assess how well the trained models generalize to new instances, providing confidence in their real-world performance.

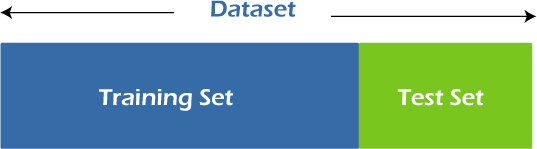


Fig 9.1 Training and Testing

## SOURCE CODE

import pandas as pd import numpy as np

import matplotlib.pyplot as plt import seaborn as sb

from sklearn.model\_selection import train\_test\_split from sklearn.ensemble import RandomForestClassifier from sklearn.neighbors import KNeighborsClassifier from sklearn.ensemble import AdaBoostClassifier from sklearn.tree import DecisionTreeClassifier

from sklearn.linear\_model import LogisticRegression

from sklearn.metrics import accuracy\_score, confusion\_matrix, classification\_report data=pd.read\_csv("online (1).csv")

data.head() data.isnull().sum() data.shape data.type.value\_counts() data.info() data.isFraud.value\_counts()

data['type']=data['type'].map({'PAYMENT':1,'CASH\_IN':2,'CASH\_OUT':3,'TRANSFER':4,'DEBIT':5}

)

data['isFraud']=data['isFraud'].map({0:'No Fraud',1:'Fraud'}) print(data.head())

data.plot()

sb.pairplot(data, hue="isFraud") plt.show() plt.hist(data['isFraud']) plt.show()

x = np.array(data[["type", "amount", "oldbalanceOrg", "newbalanceOrig"]]) y = np.array(data[["isFraud"]])

print(x) print(y)

xtrain,xtest,ytrain,ytest=train\_test\_split(x,y,test\_size=0.2) model=RandomForestClassifier()

model.fit(xtrain,ytrain) ypred=model.predict(xtest) ypred accuracy\_score(ytest,ypred)

confusion\_matrix(ytest,ypred) print(classification\_report(ytest,ypred)) model1=SVC() model1.fit(xtrain,ytrain) ypred1=model1.predict(xtest)

ypred1 accuracy\_score(ytest,ypred1) confusion\_matrix(ytest,ypred1)

print(classification\_report(ytest,ypred1)) model3=KNeighborsClassifier(n\_neighbors=7) model3.fit(xtrain,ytrain) ypred3=model3.predict(xtest)

ypred3 model4=AdaBoostClassifier(n\_estimators=7) model4.fit(xtrain,ytrain) ypred4=model4.predict(xtest)

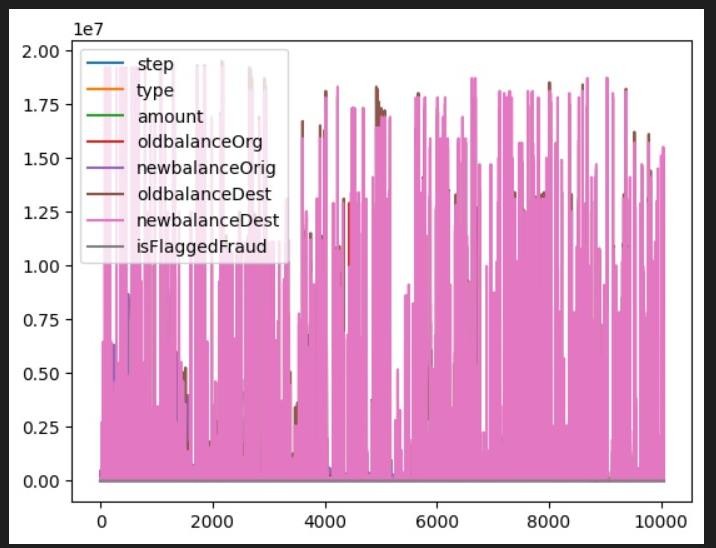
ypred4 accuracy\_score(ytest,ypred4) confusion\_matrix(ytest,ypred4)

print(classification\_report(ytest,ypred4)) model5=DecisionTreeClassifier() model5.fit(xtrain,ytrain) ypred5=model5.predict(xtest)

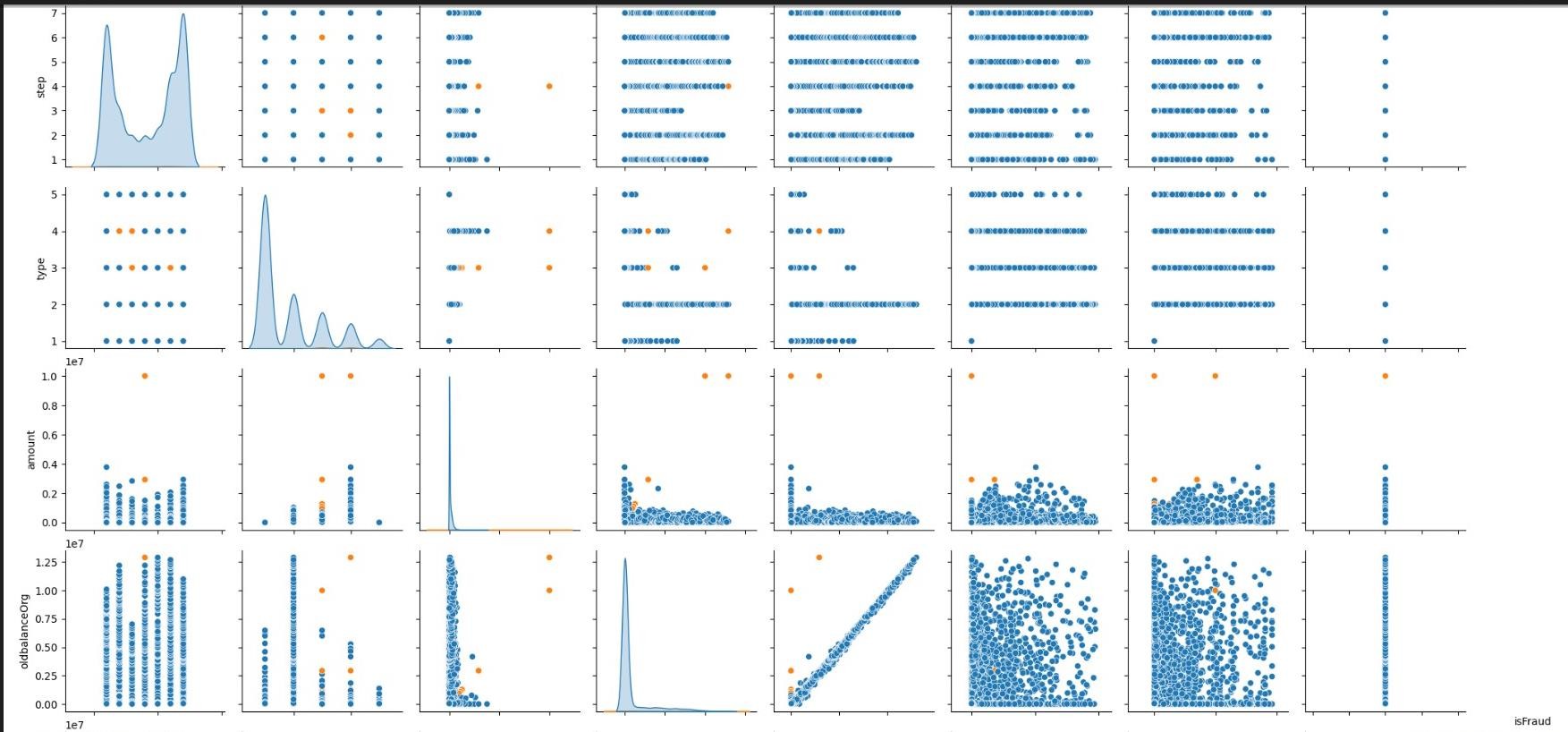
ypred5 accuracy\_score(ytest,ypred5) confusion\_matrix(ytest,ypred5)

print(classification\_report(ytest,ypred5)) model6=LogisticRegression() model6.fit(xtrain,ytrain) ypred6=model6.predict(xtest) accuracy\_score(ytest,ypred6) confusion\_matrix(ytest,ypred6) print(classification\_report(ytest,ypred6))

## VISUALIZATIONS

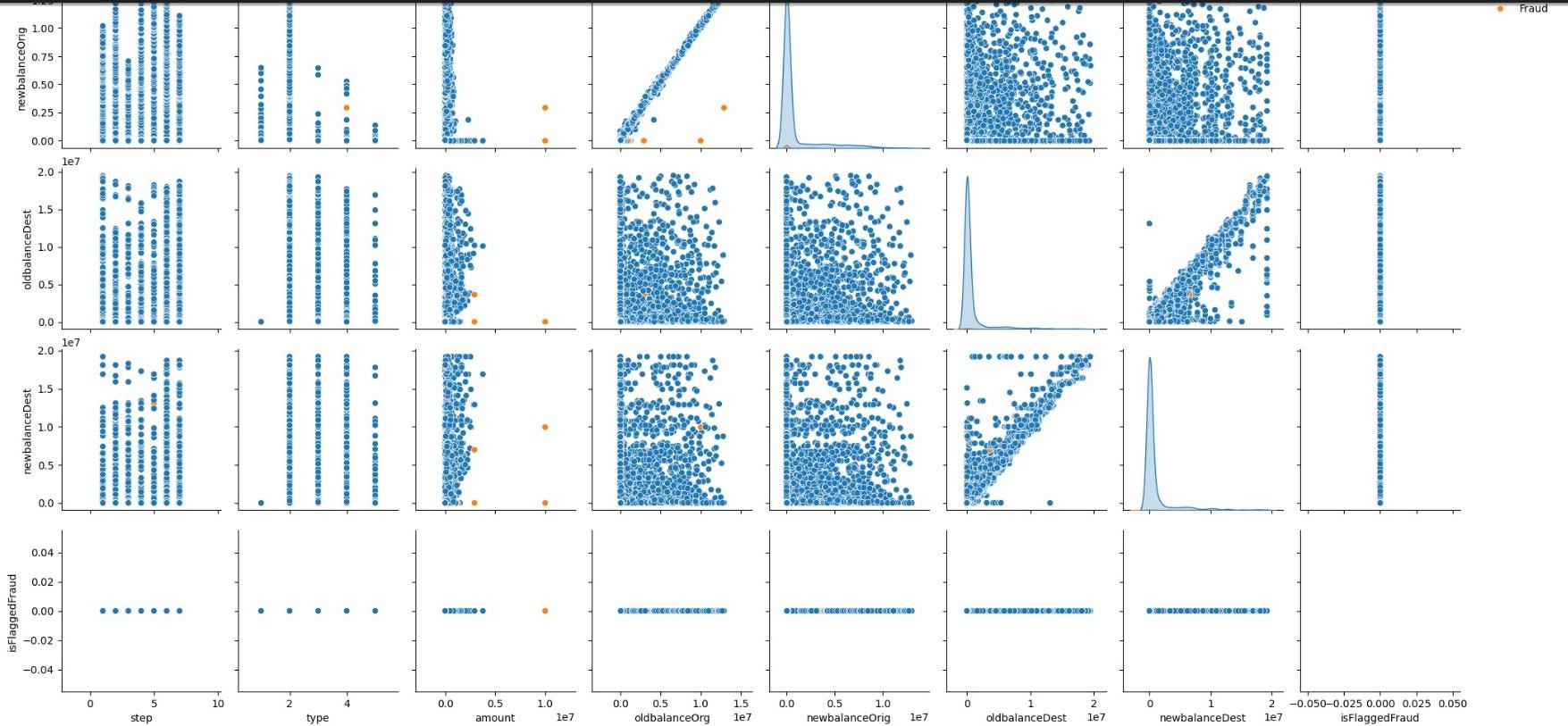


##### Fig 11.1 Plot

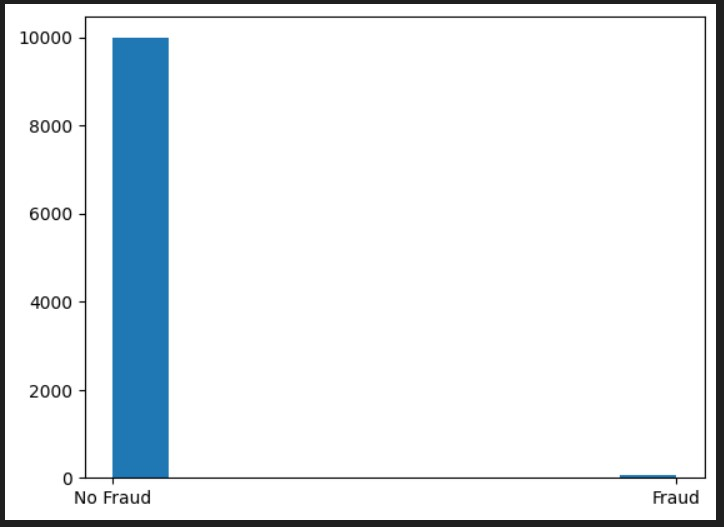


**Fig 11.2 Pairplot**

\



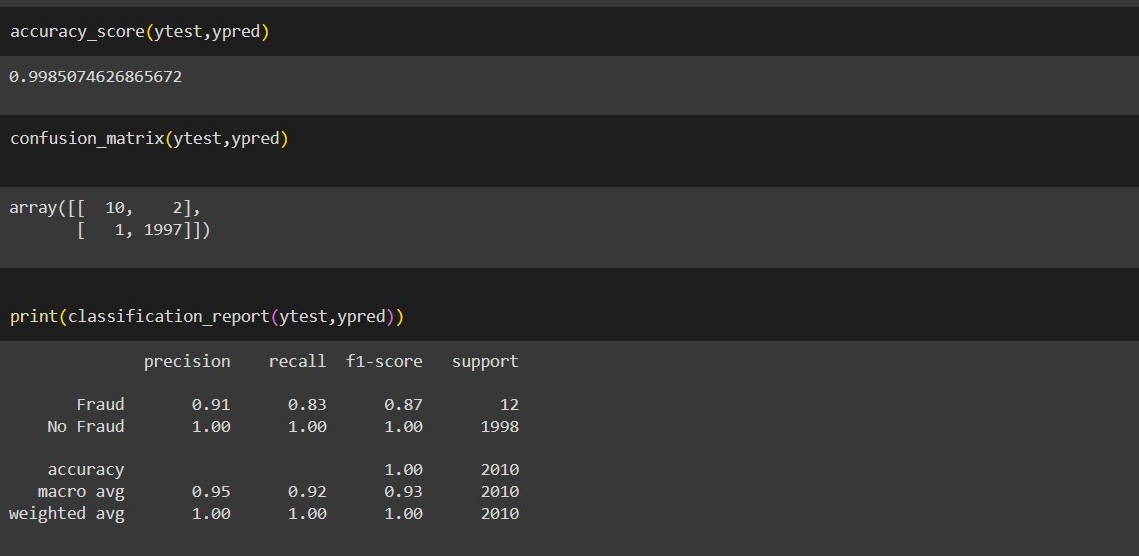
**Fig 11.3 Pairplot**



**Fig 11.4 Histogram**

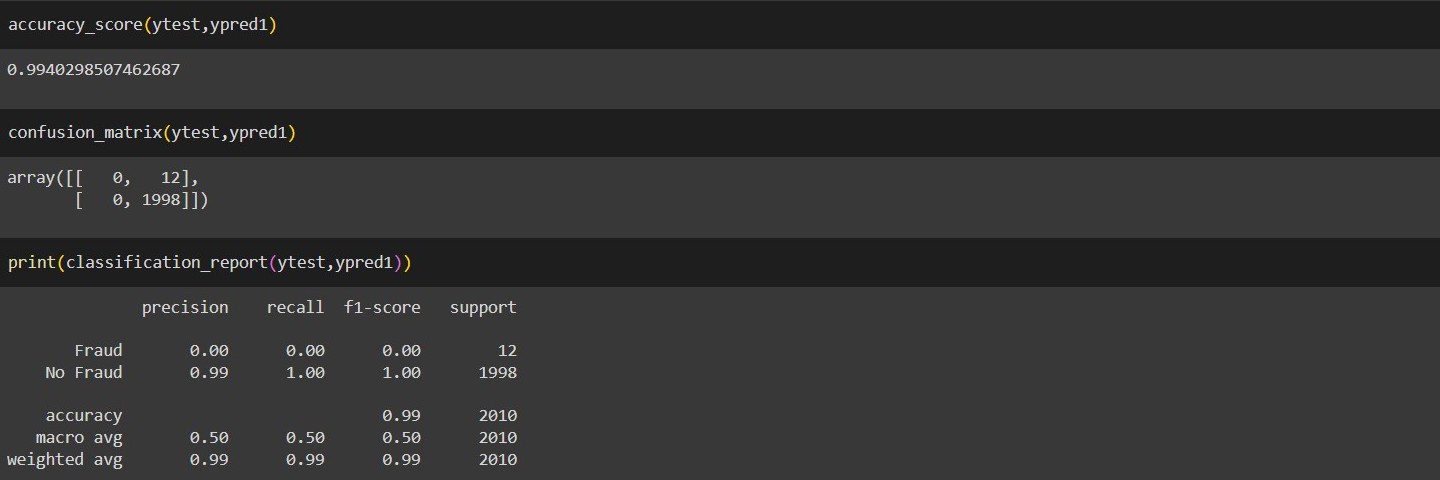
## OUTPUTS

1. **Random Forest Classifier**



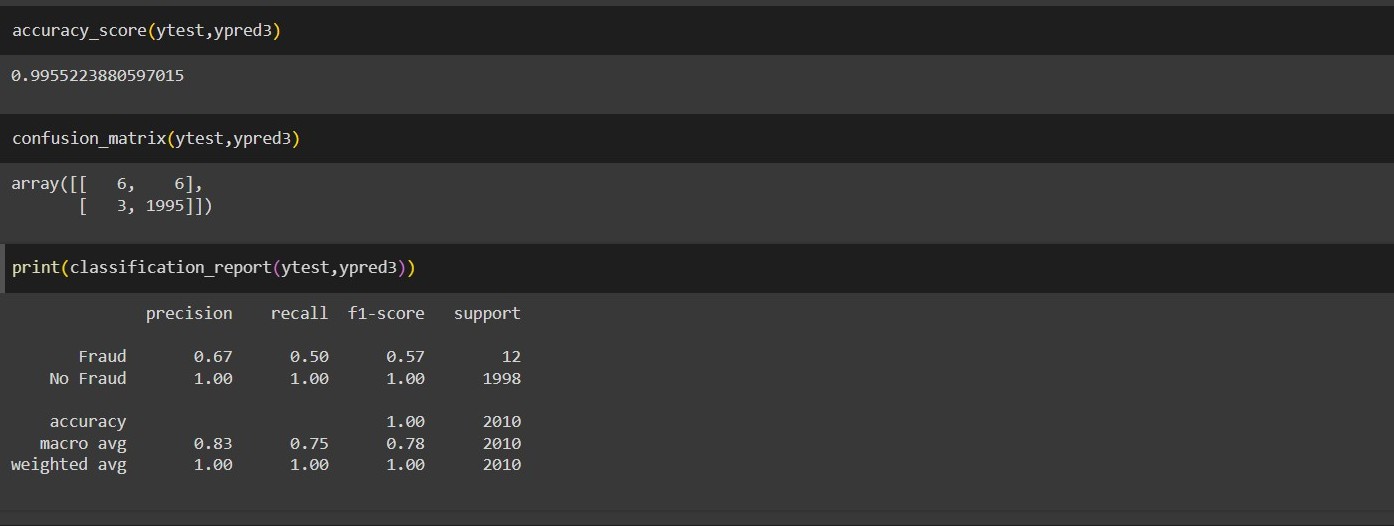
**Fig 12.1 Random Forest Classifier**

#### SVM



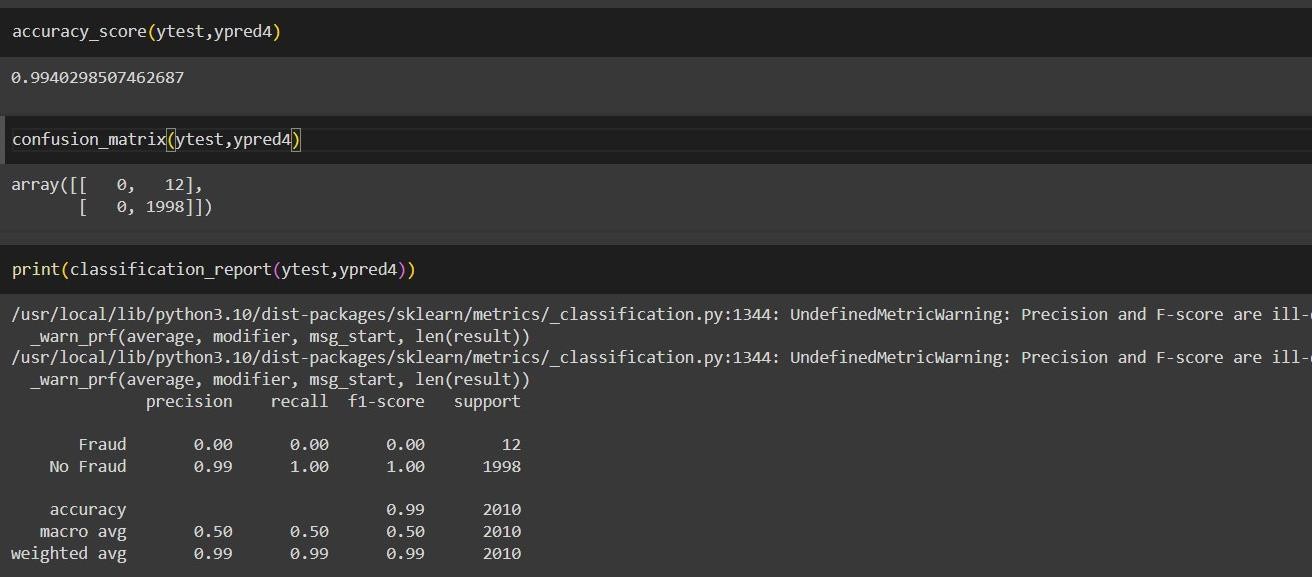
**Fig 12.2 SVM**

#### KNN



**Fig 12.3 KNN**

1. **Ada Boost Classifier**



**Fig 12.4 AdaBoost Classifier**

## CONCLUSION

Online payment fraud detection is pivotal in safeguarding digital transactions, utilizing advanced technologies like machine learning to swiftly identify and prevent fraudulent activities. By adapting to evolving fraud tactics, it ensures the integrity of online financial ecosystems and fosters trust among consumers and businesses alike. Additionally, it promotes innovation in digital commerce, supporting the widespread adoption of online payments and the growth of e-commerce platforms. In conclusion, online payment fraud detection plays a crucial role in ensuring the security and reliability of digital transactions, contributing to the stability and growth of online economies worldwide.

## FUTURE SCOPE

The fight against online payment fraud is an ongoing arms race. As fraudsters develop new techniques, so too must fraud detection systems evolve. Here's a glimpse into some less-explored areas that hold promise for the future:

1. Conversational AI and Chatbots:

Fraudulent Activity Detection via Chat Interactions: Conversational AI analysing customer service interactions can identify inconsistencies in language patterns or knowledge of account details, potentially revealing fraudulent attempts to access accounts.

Proactive Chatbot Engagement: AI-powered chatbots can proactively engage users during the payment process, clarifying unusual transactions or verifying account information, adding an extra layer of security.

1. Psychological Deception Detection:

Micro-expressions and Behavioural Analysis: Emerging technologies that analyse facial micro- expressions or voice patterns during online transactions might hold promise for detecting deception associated with fraudulent activity.

1. Quantum Computing and Cryptographic Agility:

Preparing for Post-Quantum Threats: As quantum computing advances, it could threaten the security of current encryption methods used in online payments. Research into post-quantum cryptography is crucial to ensure future-proofed security. Quantum-Resistant Fraud Detection Systems: Developing fraud detection systems that leverage the unique capabilities of quantum computing for anomaly detection and pattern recognition could be a game-changer.

These frontiers represent exciting, yet challenging, areas of exploration. By embracing these possibilities, the future of online payment fraud detection can become more sophisticated, proactive, and ultimately, more successful in safeguarding the financial ecosystem.

## REFERNCES

1. Abdulwahab Ali Almazori, Nasir Ayub‚ “Online Payment Fraud Detection Model Using Machine Learning Techniques”, IEEE, vol.11, pp. 137188-137203, ISSN: 2169-3536.
2. M. Venkatesh, Bhukya Keerthi Bai, Budati Bhargavi, Chilukoti Manasa, Dwarasala Mokshitha, “Online Payment Fraud Detection Using Machine Learning”, IJARIIE, vol.10, pp.863-867, ISSN:2395-4396
3. Mr. Ganesh Pawar, Mr. Ranapratapsingh Patil, Mr. Dinesh Sonawane, Mr. Ujval Borole, Dr. Sandip Patil, “Online Payment Fraud Detection System Using Machine Learning”, IRJMETS, Vol.06,pp.7802-7804, ISSN:2582-5208.
4. Naga Babu Pachhala, Mallipudi Devi Siva Sai Aggarwal, “Online Payment Fraud Detection”, IJISRT, vol.8, pp.1191-1195, ISSN:2456-2165.