CREDIT CARD TRANSACTION BASED ON FACE RECOGNITION TECHNOLOGY USING AI

PROJECT REPORT

Submitted by

BALA S - 811320104003

MATHIYAZHAGAN D - 811320104013

RAJESH K - 811320104019

HARIHARASUDHAN V - 811320104301

In partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

J. J. COLLEGE OF ENGINEERING AND TECHNOLOGY

TIRUCHIRAPPALLI-620009

MAY 2024

BONAFIDE CERTIFICATE

Certified that this project report "**CREDIT CARD TRANSACTION BASED ON FACE RECOGNITION TECHNOLOGY USING AI**" is the bonafide work of "**S. BALA (811320104003), K. RAJESH (811320104019), D. MATHIYAZHAGAN (811320104013), and V. HARIHARRASUDHAN (811320104301)** "who carried out the project work under my supervision. Certificate further that to the best of my knowledge the work reported here in does not form part of any other thesis or desertion on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate".

SIGNATURE

Mrs. R. SHARIFF NISHA

SUPERVISOR

Assistant professor,
Department of CSE
JJCET
Tiruchirapalli-620009

SIGNATURE

Dr. M. P. REVATHI

HEAD OF THE DEPT.

Professor,
Department of CSE
JJCET
Tiruchirapalli-620009

Submitted for Semester Project viva-voce examination held on _____

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

"Thanks" may be a little word but its eloquence is magnified only when it is spelled from the depth of the heart. At this point of time, we would like to extend our heartfelt thanks to all those who helped us throughout this major assignment.

First of all we would like to thank the "Almighty" for having given us the "Will and Determination" to pursue our goal tenaciously.

We wish to thank our college Chairman **Dr. S. Ramamoorthiy**, our college vice chairman **Mr. R. Chenthurselvan,** and our Principal **Dr. P. Mathiyalagan** for their support in completing the mini project work successfully.

We express our sincere thanks to our Head of the Department of Computer Science and Engineering, **Dr. M. P. Revathi** for the support in completing the work successfully.

With extreme sense of gratitude, we express our sincere thanks to our project guide **Mrs. R. Shariff Nisha** and project coordinator **Dr. S. Venkatesh** and all the faculty Members of the CSE Department for giving valuable guidance, immense help and their encouragement throughout our project work.

We owe our most genuine thanks to our beloved parents, siblings and friends for their continuous support

ABSTRACT

In real time payment modes have different modes such as cash on delivery, online transaction, credit card transaction and monthly installments etc. Whenever online transactions take place, the customer involves option for credit/debit cards or internet banking. As we know, during online transactions there are many chances to steal the confidential information by the attackers or hackers. So implement the framework to recognize the face using Grassmann algorithm at the time of transactions with improved accuracy rate and also post the complaints about unknown person access at the time of transactions.

The Credit Card fraud identification project distinguishes the deceitful idea of the new exchange by shaping the credit card exchanges with the information on those which have been fake. To distinguish, in an event exchange is a typical transaction which can be real or fraud. A predictive model is employed for detection of cheat and legitimate exchanges using a popular machine learning algorithm called Random Forest Algorithm. This model is designed to validate each transaction of the credit card accurately. The algorithm is designed such that it will analyze the data efficiently.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

POS	-	POINT OF SALES
DFD	-	DATA FLOW DIAGRAM
HTML	-	HYPER TEXT MARKUP LANGUAGE
RF	-	RANDOM FOREST
LR	-	LOGISTIC REGRESSION
GBT	-	GRADIENT BOOSTED
LSTM	-	LONG SHORT TERM MEMORY
SVM	-	SUPPORT VECTOR MACHINE

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION ABOUT CREDIT CARD TRANSACTION AND ARTIFICIAL INTELLIGENCE

Money is an important thing in this world. The payment modes at Point of Sales (POS) have different modes such as cash on delivery, online transaction, credit card transaction and monthly instalments etc. Whenever online transactions take place, the customer involves option for credit/debit cards or internet banking. The credit card provides prominent use of payment method, so it is followed in many scenarios. In real time, during online transactions there are many chances to steal the confidential information by the attackers or hackers.

The information is processed and the acknowledgement is sent to the bank for both the valid and invalid transactions**.** A method for credit card transaction system which will make use of face recognition and face detection technology using web application. The main problem faced by credit card user is attack to lot of privacy issues such as credit card. This generally happens when users give their credit card to unknown people or when the card is lost. So, here processing a system that will reduce the risk of credit card frauds.

This system processing input face image and match the user's face image with dataset of respective user. A database will be maintained for the authentication purpose. This proposed method utilizes the properties of Grassmann learning algorithm for face recognition during transaction process. If the images matches, that means user is genuine and he will allow to process otherwise, the user will be denied to do the transaction. As a global society, we have quite come far from the barter system, cash, debit and credit cards and now e-commerce. These ever-developing techniques of money transactions benefit us in lot many ways. They make day-to-day life smooth. Millions of dollars are transacted each day over the world for different purposes. But

apart from easing our lives, a money transaction can prove to be dangerous if it becomes a victim of a fraudulent activity. Fraud is a deception done with the intent to gain illegitimate financial profit. Some of the ways the frauds take place include- hacking billing devices at shops or restaurants, hacking an e-commerce merchant, lost or theft cards and fraud devices fitted in card readers in gas stations or ATMs to steal the PIN numbers of credit cards. A survey held in 2012, shows that the companies lost an average of 0.9% of their online revenue to frauds. Using the industry market database of North America, it was estimated that nearly 3.5 billion dollars was lost to frauds . To avoid fraudulent transactions, it is necessary to detect them precisely. But detecting a fraudulent transaction is a very complex problem since the fraud transactions are very less in number and do not follow the same pattern.

1.2 DATASET DESCRIPTION

The dataset contains the details of some European credit card holders recorded in September 2013. The dataset comprises the transaction information for two days, which has 492 fraud transactions out of 284,807 transactions. For security purposes, the features of the dataset are not revealed. Instead, the PCA values of the features are given. A PCA is a technique to get a low dimensional structure out of a potential high dimensional dataset. It includes the extraction of q eigenvectors for q input distribution. It is one of the most used algorithm for dimensionality reduction. The basis vectors are known as principal components. The dataset contains a total of 31 columns of which, 28 are PCA components named as V1, V2….V28. Moreover, the time and amount of the money transaction has also been provided. The target variable classifies a transaction as 0 for valid transaction and 1 for fraudulent transaction.

1.3 DATASET PRE-PROCESSING

The dataset contains only 492 fraud transactions of 284,807 transactions, which leads to the dataset being highly imbalanced. An imbalanced dataset can result in faulty predictions. To solve this problem, we used two approaches in this paper. The first approach involved resampling the dataset to increase the number of fraudulent

transactions to make it proportional. Resampling is a technique that involves extracting repeated samples from the original datasets. The second approach we used was to apply weights to the classifiers to emphasize the effect of fraudulent transactions in the prediction system.

1.4 METHOD DESCRIPTION

Most of the commonly used models in deep learning use the ANN as a full connection layer in some or the other form which makes it the most fundamental neural network. They have found various uses in applications such as speech recognition , facial recognition , character recognition , etc. The architecture of an ANN which can be divided into 3 major parts: the output, hidden and the input layers. Directed, weighted connections are made between each layer's nodes, the weights which are adjusted while training.

1.5 CARD TYPES AND ATTRIBUTES

A multitude of credit card products are available to consumers, and the number of products is growing. Terms and conditions of each credit card product offered, such as the Annual Percentage Rate (APR) , the monthly minimum payment formula, and certain fees, are detailed in a cardholder agreement which is required by regulation. The following sections provide an overview of some common credit card product categories.

GENERAL PURPOSE CREDIT CARDS

General purpose, or universal, credit cards can be used at a variety of stores and businesses. They take on many forms, including standard, premium, affinity, co-branded, corporate, home equity, and cash secured programs, each of which is briefly described next.

STANDARD CREDIT CARD PROGRAMS

Standard credit card programs are a traditional form of credit card issuance. These

programs are usually marketed to consumers who meet or exceed the institution's minimum credit criteria but that may lack sufficient credit history or may fail to meet some of the institution's other credit criteria. Due to the higher credit risk and loss rates, these programs generally carry higher interest rates, higher fees, and lower credit limits than premium credit card programs. In addition to cash secured credit cards (discussed later), unsecured standard credit card programs are frequently used for providing credit to subprime borrowers.

PREMIUM CREDIT CARD PROGRAMS

Premium credit card programs tend to be marketed to consumers that have higher income and/or higher credit scores than those consumers offered standard credit cards. Premium programs have traditionally consisted of gold and platinum credit cards. However, some issuers have moved toward using these premium-sounding titles with more standard-type products to combat strong competition and entice consumers to opt for their cards. Premium credit card programs usually carry lower interest rates, waived annual fees, and higher credit limits. The risk with this type of program is a large volume of high-balance accounts. Over-reliance on the premium sector creates the potential of greater losses in the event high outstanding balances exist during an economic downturn.

AFFINITY CREDIT CARD PROGRAMS:

Affinity relationships are partnerships formed between financial institutions and unaffiliated groups (affinity partners), generally nonprofit organizations such as, but not limited to, alumni associations, professional organizations, and fan clubs. A contractual agreement governs the relationship with the affinity partner, and the affinity cards issued usually carry the affinity partner's logo.

Compensation varies, but the affinity partner endorsing the card usually receives financial compensation based on the projected level of acceptance and use by its members. Compensation often comes in the form of the sharing of annual fees, renewal fees, interchange income, and interest income.

CO-BRANDED CREDIT CARD PROGRAMS:

Co-branded relationships are partnerships formed between financial institutions and unaffiliated organizations, generally for-profit organizations such as airlines, automobile manufactures, and retailers. Similar to the affinity program, a contractual agreement governs the co-branded relationship, and the co-branded card usually carries the co-branded partner's logo. Compensation to the co-branding partner often takes the form of sharing interchange fees and/or rebates to its customers. Rebates to customers are normally based on a percentage of purchases or transactions, and the percentage often varies depending on whether purchases were made with the co-branding party or another entity.

The institution benefits from a cobranding arrangement because it generally increases credit card receivables, and accordingly interest and interchange income, due to the consumers' willingness to use the credit card more frequently to reap the financial rewards. However, institutions typically face the risk that higher cardholder monthly payment rates could erode profits. Nevertheless, for some programs the considerable volume of interchange income generated by high cardholder transaction volumes might substantially offset the interest income opportunity that is lost with higher payment rates.

1.6 FRAUD PREVENTION TECHNOLOGIES

While fraudsters are using sophisticated methods to gain access to credit card information and perpetrate fraud, new technologies are available to help merchants to detect and prevent fraudulent transactions. Fraud detection technologies enable

merchants and banks to perform highly automated and sophisticated screenings of incoming transactions and flagging suspicious transactions. While none of the tools and technologies presented here can by itself eliminate fraud, each technique provides incremental value in terms of detection ability. As it will be discussed later, the best practice implementations often utilize several of these fraud prevention techniques, if not all of the tools discussed here. The various fraud prevention techniques are discussed below:

MANUAL REVIEW

This method consists of reviewing every transaction manually for signs of fraudulent activity and involves a exceedingly high level of human intervention. This can prove to be very expensive, as well as time consuming. Moreover, manual review is unable to detect some of the more prevalent patterns of fraud, such as use of a single credit card multiple times on multiple locations (physical or web sites) in a short span.

ADDRESS VERIFICATION SYSTEM

This technique is applicable in card-not-present scenarios. Address Verification System (AVS) matches the first few digits of the street address and the ZIP code information given for delivering/billing the purchase to the corresponding information on record with the card issuers. A code representing the level of match between these addresses is returned to the merchant. AVS is not much useful in case of international transactions.

1.7 RECENT DEVELOPMENTS IN FRAUD MANAGEMENT

The technology for detecting credit card frauds is advancing at a rapid pace – rules based systems, neural networks, chip cards and biometrics are some of the popular techniques employed by Issuing and Acquiring banks these days. Apart from technological advances, another trend which has emerged during the recent years is that fraud prevention is moving from back-office transaction processing systems to

front-office authorization systems to prevent committing of potentially fraudulent transactions. However, this is a challenging trade-off between the response time for processing an authorization request and extent of screening that should be carried out.

SIMPLE RULE SYSTEMS

Simple rule systems involve the creation of 'if...then' criteria to filter incoming authorizations /transactions. Rule-based systems rely on a set of expert rules designed to identify specific types of high-risk transactions. Rules are created using the knowledge of what characterizes fraudulent transactions. For instance, a rule could look like – If transaction amount is > $5000 and card acceptance location = Casino and Country = 'a high-risk country'. Fraud rules enable to automate the screening processes leveraging the knowledge gained over time regarding the characteristics of both fraudulent and legitimate transactions. Typically, the effectiveness of a rule-based system will increase over time, as more rules are added to the system. It should be clear, however, that ultimately the effectiveness of the system depends on the knowledge and expertise of the person designing the rules.

RISK SCORING TECHNOLOGIES

Risk scoring tools are based on statistical models designed to recognize fraudulent transactions, based on a number of indicators derived from the transaction characteristics. Typically, these tools generate a numeric score indicating the likelihood of a transaction being fraudulent: the higher the score, the more suspicious the order. Risk scoring systems provide one of the most effective fraud prevention tools available. The primary advantage of risk scoring is the comprehensive evaluation of a transaction being captured by a single number. While individual fraud rules typically evaluate a few simultaneous conditions, a risk-scoring system arrives at the final score by weighting several dozens of fraud indicators, derived from the current transaction attributes as well as cardholder historical activities. E.g., transaction amounts more than three times the average transaction amount for the cardholder in the last one year.

NEURAL NETWORK TECHNOLOGIES

Neural networks are an extension of risk scoring techniques. They are based on the 'statistical knowledge' contained in extensive databases of historical transactions, and fraudulent ones in particular. These neural network models are basically 'trained' by using examples of both legitimate and fraudulent transactions and are able to correlate and weigh various fraud indicators (e.g., unusual transaction amount, card history, etc) to the occurrence of fraud.

1.8 PROPRIETARY CREDIT CARDS

Proprietary cards, also called private label cards, are issued under a contractual agreement between financial institutions and third parties, usually large retailers, for the purpose of consumers transacting business with that entity. Some are also issued by the retailers and do not involve a financial institution. Private label cards often exhibit different traits than general purpose cards in that private label cards normally have lower credit limits, higher interest rates, higher credit risk profiles, and limited use (for example, limited to a particular merchant).

There is risk of the retail partner failing. While significant direct exposure to the company may not be evident, high losses may still result if cardholders do not feel compelled to repay outstanding balances. Some customers may not honor obligations due to lost warranties or rights to return merchandise. Others might not repay the debt simply because the merchant is no longer in business. In either case, the bankruptcy of a retail partner usually creates a significant collection problem. In addition, credit risk is closely correlated with the traits of the cardholder population which are usually small, niche markets tending to have volatile performance patterns. The credit quality of these populations also tends to be lower because there is generally an incentive to establish liberal underwriting standards and enroll as many applicants as possible to generate business for the retail partner.

CASH ACCESS CREDIT CARDS

Cash access credit cards are marketed to consumers who tend to prefer cash advances over purchases. These cards are not used for traditional point-of-sale transactions. Cash-users are typically considered a higher-risk population. In some cases these borrowers may be using cash advances to pay debts, including balances on this or other credit cards (this can also be true for some borrowers who use cash advance features of their general purpose cards).

OTHER TYPES OF BANKCARDS

Not all cards issued by banks are credit cards. For example, banks also issue debit cards and prepaid or stored value cards. Examples of stored-value cards include payroll cards, electronic benefits transfer (EBT) cards, travel fund cards, and store gift cards. This manual focuses on credit cards.

1.9 ARTIFICIAL INTELLIGENCE AND THE FUTURE

It is said that AI is the greatest thing humankind has ever worked on. AI is being used in image and speech recognition and analysis which will be far better than human recognition of image and speech and its application stretches wide and far. There are research and works being conducted using AI that is going to play a very important role in our future healthcare. AI is being worked on to cure Alzheimer's disease and someday even blindness. Someone with dyslexia is being helped to read better with the help of AI. Genetic data is being analyzed by bioinformatics; data science integrated with AI for way better data analysis in healthcare that has not been possible for us in the past.

Fields like cancer research and other such diseases are being impacted greatly by advanced applications of AI. AI can be a great tool in the future of education. AI can be used to analyze data from an individual's personal and intellectual needs, capabilities, choices and limitations to develop customized curriculum, strategies and

schedules that will be more well suited, appealing and inclusive of most, if not all, children and adults.

SUPERVISED LEARNING:

Supervised learning is a process where our machines are designed to learn with the feeding of labelled data. In this process our machine is being trained by giving it access to a huge amount of data and training the machine to analyze it. For instance, the machine is given a number of images of dogs taken from many different angles with color variations, breeds and many more diversity. So that, the machine learns to analyze data from these diverse images of dogs and the "insight" of machines keep increasing and soon the machine can predict if it's a dog from a whole different picture which was not even a part of the labelled data set of dog images the machine was fed earlier.

UNSUPERVISED LEARNING:

Contrary to the supervised learning, the unsupervised learning algorithms comprises analyzing unlabelled data i.e., in this case we are training the machine to analyze and learn from a series of data, the meaning of which is not apparently comprehendible by the human eyes. The machine looks for patterns and draws conclusions on its own from the patterns of the data. Important thing to remember that the dataset used in this instance is not labelled and the conclusions are drawn by the machines.

REINFORCEMENT LEARNING:

Reinforcement learning is a feedback dependent machine learning model. In this process the machine is given a data and made to predict what the data was. If the machine generates an inaccurate conclusion about the input data, the machine is given feedback about its incorrectness. For example, if you give the machine an image of a basketball and it identifies the basketball as a tennis ball or something else, you give a negative feedback to the machine and eventually the machine learns to identify an image of a basketball on its own when it comes across a completely different picture

of a basketball. Deep Learning, on the other hand is the concept of computers simulating the process a human brain takes to analyze, think and learn. The deep learning process involves something called a neural network as a part of the thinking process for an AI. It takes an enormous amount of data to train deep learning and a considerably powerful computing device for such computation methods.

1.10 CONCERNS ABOUT AI

One of the most immediate concerns about Artificial Intelligence is the fear of losing jobs. Artificial Intelligence enhancing automation is also causing huge job losses around the world. According to a Forbes article, it is predicted that by 2025 automation will cause a loss of 85 million jobs. Bigger fears regarding AI includes the scenario whereas machines become smarter and smarter they going to end up being as opinionated and biased like some of the people training it. Automation of weapons is also a big reason people worry about the future of Artificial Intelligence.

The idea that weapons can be used to search and target someone with pre-programmed instructions and the misuse of this by governments or mafias or rogue AI can be something very deadly and devastating. However, there are many myths in disguise of concerns surrounding AI that spreads panic and misinformation. AI today is nowhere near to become a super-intelligent entity and turn into our overlords like in sci-fi movies. However, heavy regulations and cautions are being advised by Big Tech giants like Elon Musk while developing this industry.

CHAPTER 2

LITERATURE SURVEY

2.1 A DUAL APPROACH FOR CREDIT CARD FRAUD DETECTION USING NEURAL NETWORK AND DATA MINING TECHNIQUES

Authors & Year: Sahu, Aanchal, G. M. Harshvardhan, and Mahendra Kumar Gourisaria – 2022.

The world is being more and more digitalized with each passing day, making information security a huge concern. Through efficient fraud detection using a robust approach, the banking industry will be able to avert fraudulent transactions and save millions of dollars every year. Each money transaction is crucial and thus, fraudulent transactions need to be detected at any cost. In this paper, we build models to detect fraudulent credit card transactions using five classifiers to find out the best fit classifier for the situation. We use two different techniques to tackle the inherent problem of data imbalance. The first technique uses data resampling technique to increase the number of samples in the minority class, whereas, the second one uses a cost-based approach where the error function incorporates weights of each class. Through the weights, more emphasis can be given to the samples of fraudulent transactions than the normal samples.

2.2 CREDIT CARD FRAUD DETECTION THROUGH MACHINE LEARNING ALGORITHM

Authors & Year : Panda, Agyan, Bharath Yadlapalli, and Zhi Zhou – 2022.

Fraudsters are now more active in their attacks on credit card transactions than ever before. With the advancement in data science and machine learning, various algorithms have been developed to determine whether a transaction is fraudulent. We study the performance of three different machine learning models: logistic regression, random forest, and decision trees to classify, predict, and detect fraudulent credit card

transactions. We compare these models' performance and show that random forest produces a maximum accuracy of 96% (with an area under the curve value of 98.9%) in predicting and detecting fraudulent credit card transactions. Thus, we recommend random forest as the most appropriate machine learning algorithm for predicting and detecting fraud in credit card transactions.

2.3 CREDIT CARD FRAUD DETECTION USING SUPPORT VECTOR MACHINE

Authors & Year : Kumar, Sheo, Vinit Kumar Gunjan, Mohd Dilshad Ansari, and Rashmi Pathak – 2022.

It is certain that with the advent of deregulation liberalization, globalization and privatization new ways are opened for banks to enhance their revenues by diversifying their product portfolio and offerings. Technology is going to be a major player in enhancing customer delight and a place to provide uniform and integrated banking services to its clients. In fact, all major World Corporations are in the process of procuring and implementing advanced technologies with changing times and banking is no exception to this. Banks are spending considerable amount of time to spread awareness and allocating funds for the same along with offering schemes on the purchase of products/payment through banking app linked with Debit/Credit Cards like cash backs and discounts. With the focus of the Indian Government to curb the menace of black money and use of plastic money from one's account, the usage of mobile banking shall keep rising and more customers would choose the same over traditional banking.

2.4 CREDIT CARD FRAUD DETECTION SYSTEMS (CCFDS) USING MACHINE LEARNING (APACHE SPARK)

Authors & Year : Vinaya, D. S., Satish B. Basapur, Vanishree Abhay, and Neetha Natesh – 2023

As the payment method is simplified by the combination of the financial industry and IT technology, the payment method of consumers is changing from cash payment to electronic payment using credit card, mobile micropayment, and app card. As a result, the number of cases in which anomalous transactions are attempted by abusing e-banking has increased and financial companies started establishing a Fraud Detection System (FDS) to protect consumers from abnormal transactions. The abnormal transaction detection system aims to identify abnormal transactions with high accuracy by analyzing user information and payment information in real time. Although FDS has shown good results in reducing fraud, but the majority of cases being flagged by this system are False Positives that resulting in substantial investigation costs and cardholder inconvenience. The possibilities of enhancing the current operation constitute the objective of this research. Based on variations and combinations of testing and training class distributions, experiments were performed to explore the influence of these parameters. In this study, we investigated the trend of abnormal transaction detection using payment log analysis and data mining, and summarized the data mining algorithm used for abnormal credit card transaction detection. We used python programming with Apache spark for advanced processing of data and high accuracy.

2.5 CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING: A SURVEY

Authors & Year : Lucas, Yvan, and Johannes Jurgovsky – 2023.

Nowadays digitalization gaining popularity because of seamless, easy and convenience use of e-commerce. It became very rampant and easy mode of payment. People choose online payment and e-shopping; because of time convenience, transport convenience, etc. As the result of huge amount of e-commerce use, there is a vast

increment in credit card fraud also. Fraudsters try to misuse the card and transparency of online payments. Thus to overcome with the fraudsters activity become very essential. The main aim is to secure credit card transactions; so people can use e-banking safely and easily. To detecting the credit card fraud there are various techniques which are based on Deep learning, Logistic Regression, Naive Bayesian, Support Vector Machine (SVM), Neural Network, Artificial Immune System, K Nearest Neighbor, Data Mining, Decision Tree, Fuzzy logic based System, Genetic Algorithm.

CHAPTER 3

PROBLEM DEFINITION

3.1 EXISTING SYSTEM

In credit card transaction method, the cardholder physically presents his card to the merchant for payment. An attacker must steal the credit or debit card in order to carry any fraudulent activity in this type of purchase. If the cardholder does not notice the theft of the card, the credit card firm may suffer a significant financial loss. Only a few key details about credit card information (card number, expiration date, and security code) are necessary to complete the transaction. Typically, such purchases are made over the phone or on the Internet. A scammer only has to have the card details to conduct fraud in such types of transactions. Almost all of the times, the actual cardholder is unaware that his or her card information has been seen or stolen by someone else. Detection of fraud based on an examination of a cardholder's existing purchase data is a promising method of reducing the percentage of successful fraudulent activity.

Existing system introduces an innovative framework that amalgamates feature vectors from the Ensemble Auto encoder and ResNeXt (EARN). EARN offers the advantage of effectively capturing both high-dimensional and low- dimensional features in financial transaction data. This approach leverages the collective learning from multiple feature extraction methods, to create a unified, comprehensive feature representation. This vector becomes a powerful asset in enhancing the model's ability to discern meaningful patterns in financial transaction data. RXT classification model designed to navigate big data's complexities while maintaining exceptional accuracy in distinguishing between normal and fraudulent financial transactions.

DISADVANTAGES

- Existing models haven't been widely used in fraud detection of credit card fraud.
- This method may require significant computational resources and its performance can vary depending on the dataset.
- It only focuses on dataset based fraud classification, does not avoid the fraudulent activities.
- Need to enhance the application for real time fraud analysis in credit card transactions.

3.2 DATA DICTIONARY

Table Name: Admin Table

Table 3.1 Admin table

Field	Type	Null	Defaul t
Username	varchar(250)	Yes	NULL
Password	varchar(250)	Yes	NULL

Table Name: Booking Table

Table 3.2 Booking table

Field	Type	Null	Default
Id	Big-int(250)	Yes	NULL
Book-id	varchar(250)	Yes	NULL
Product-Id	varchar(250)	Yes	NULL
ProductName	varchar(250)	Yes	NULL
UserName	varchar(250)	Yes	NULL
Mobile	varchar(250)	Yes	NULL
Email	varchar(250)	Yes	NULL
Qty	varchar(250)	Yes	NULL
Amount	decimal(18,0)	Yes	NULL

CardType	varchar(250)	Yes	NULL
CardNo	varchar(250)	Yes	NULL
Cvno	varchar(250)	Yes	NULL
Date	varchar(250)	Yes	NULL
Status	varchar(250)	Yes	NULL

Table Name: Cart Table

Table 3.3 Cart table

Field	Type	Null	Default
Id	bigint(10)	Yes	NULL
UserName	varchar(250)	Yes	NULL
CardNo	varchar(250)	Yes	NULL
CardType	varchar(250)	Yes	NULL
ExpiryMonth	varchar(250)	Yes	NULL
ExpiryYear	varchar(250)	Yes	NULL
CvNo	varchar(250)	Yes	NULL
Pin	varchar(250)	Yes	NULL
Status	varchar(50)	Yes	NULL

Table Name: Product Table

Table 3.4 Product table

Field	Type	Null	Default
ProductId	varchar(250)	Yes	NULL
Gender	varchar(250)	Yes	NULL
Category	varchar(250)	Yes	NULL
SubCategory	varchar(250)	Yes	NULL
Product Type	varchar(250)	Yes	NULL
Colour	varchar(250)	Yes	NULL
Usage	varchar(250)	Yes	NULL
Product Title	varchar(250)	Yes	NULL
Image	varchar(250)	Yes	NULL
Image URL	varchar(1000)	Yes	NULL

Table Name: Register Table

Table 3.5 Register table

Field	Type	Null	Default
Name	varchar(250)	Yes	NULL
Gender	varchar(250)	Yes	NULL
Age	varchar(20)	Yes	NULL
Email	varchar(250)	Yes	NULL
Mobile	varchar(250)	Yes	NULL
Address	varchar(250)	Yes	NULL
UserName	varchar(250)	Yes	NULL

Password	varchar(250)	Yes	NULL

Table Name: Review Table

Table 3.6 Review table

Field	Type	Null	Default
Id	bigint(250)	Yes	NULL
ProductId	varchar(250)	Yes	NULL
ProductType	varchar(250)	Yes	NULL
ProductName	varchar(250)	Yes	NULL
Price	varchar(250)	Yes	NULL
Image	varchar(500)	Yes	NULL
UserName	varchar(250)	Yes	NULL
Rate	bigint(250)	Yes	NULL
Review	varchar(500)	Yes	NULL
Result	varchar(250)	Yes	NULL

Table Name: Temp Table

Table 3.7 Temp table

Field	Type	Null	Default
Id	bigint(20)	Yes	NULL
UserName	varchar(250)	Yes	NULL
Number	varchar(250)	Yes	NULL

DATA DICTIONARY

Table 3.8 Data dictionary

Field	Type	Constraints	Sample Values
Id	int(10)	It describes the id of user	1267454

Name	varchar(250)	It describes the name of the user	John
Gender	varchar(250)	It describes the gender of theuser	Male
Age	varchar(250)	It describes the age of the user	25
Email	varchar(250)	It describes the email id	John@gmail.com
Mobile	varchar(250)	It describes the mobile number	9876543210
Address	varchar(250)	It describes the address of the user	Trichy
UserNam	varchar(250)	It describes the username	John
Password	varchar(250)	It describes the password	********
ProductId	varchar(250)	It describes the product Id	8799
ProductType	varchar(250)	It describes the product type	Girls Wear
ProductName	varchar(250)	It describes the product name	Top Wear
Price	varchar(250)	It describes the price	2000
Image	varchar(500)	It describes the image	C:proj//sampleimage
Review	varchar(500)	It describes the review	Good
Result	varchar(250)	It describes the result	3 star
Result	varchar(250)	It describes the result	29.03.2024
Result	varchar(250)	It describes the IFSC code	SBI0003121
Category	varchar(250)	It describes the category	Dress
SubCategory	varchar(250)	It describes the sub category	Girls Wear
ProductType	varchar(250)	It describes the product type	Top Wear

Colour	varchar(250)	It describes the color	Red
Usage	varchar(250)	It describes the usage	Top Wear
CardNo	varchar(250)	It describes the card number	889874349
CardType	varchar(25	It describes the card type	Credit

	0)		

ExpiryMonth	varchar(250)	It describes the expiry month	12
ExpiryYear	varchar(250)	It describes the expiry year	2027

CvNo	varchar(250)	It describes the CV number	ISSS98378
Pin	varchar(250)	It describes the PIN number	7654
Status	varchar(50)	It describes the status	0

3.3 SYSTEM DESIGN / LOGICAL DEVELOPMENT

DATA FLOW DIAGRAM

A two-dimensional diagram explains how data is processed and transferred in a system. The graphical depiction identifies each source of data and how it interacts with other data sources to reach a common output. Individuals seeking to draft a data flow diagram must identify external inputs and outputs, determine how the inputs and outputs relate to each other, and explain with graphics how these connections relate and what they result in. This type of diagram helps business development and design teams visualize how data is processed and identify or improve certain aspects.

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

DFD LEVEL 0

The Level 0 DFD shows how the system is divided into 'sub-systems' (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be present in order for the system to do its job, and shows the flow of data between the various parts of the system.

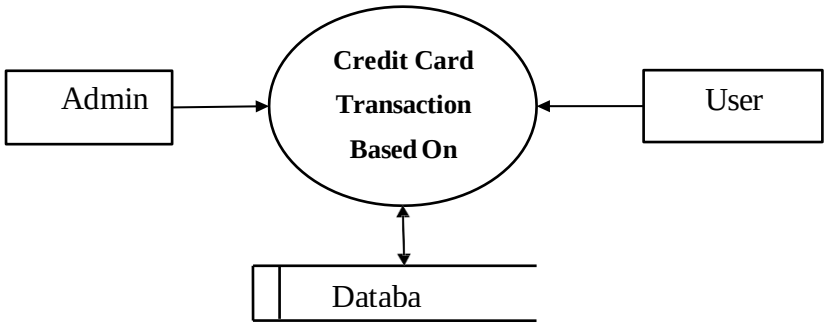


Figure 3.1 Data flow diagram level 0

DFD LEVEL-1

The next stage is to create the Level 1 Data Flow Diagram. This highlights the main functions carried out by the user. As a rule, to describe the system was using between two and seven functions - two being a simple system and seven being a complicated system. This enables us to keep the model manageable on screen or paper.

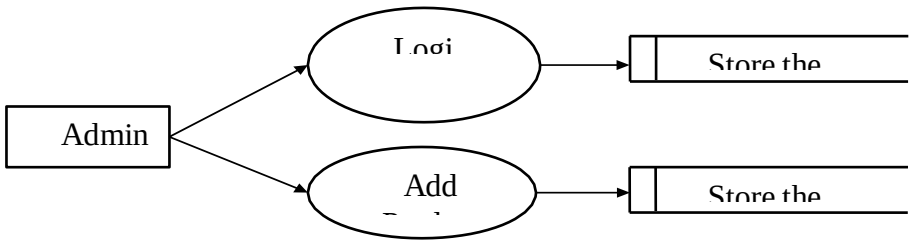


Figure 3.2 Data flow diagram level 1

DFD LEVEL-2

The next stage is to create the Level 2 Data Flow Diagram. This highlights the main functions carried out by the administrator of the system. As a rule, to describe the system was using between two and seven functions - two being a simple system and seven being a complicated system. This enables us to keep the model manageable on screen or paper.

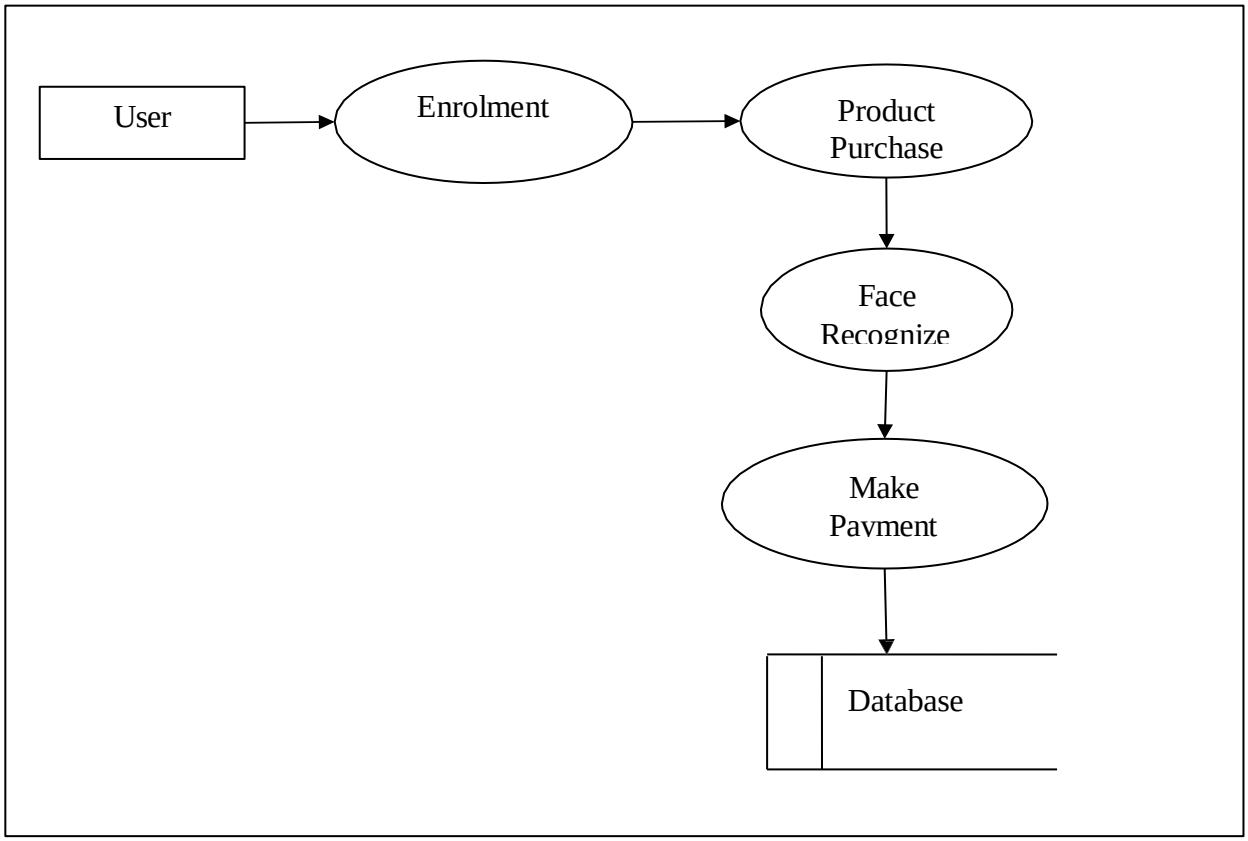


Figure 3.3.3 Data flow diagram level 2

USE CASE DIAGRAM

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved. The purpose of the use case diagram is to capture the dynamic aspect of a system. Use case diagrams are used to gather the requirements of a system including internal and external influences. These requirements are mostly design requirements. Hence, when a system is analyzed to gather its functionalities, use cases are prepared and actors are identified. The purposes of use case diagrams are –

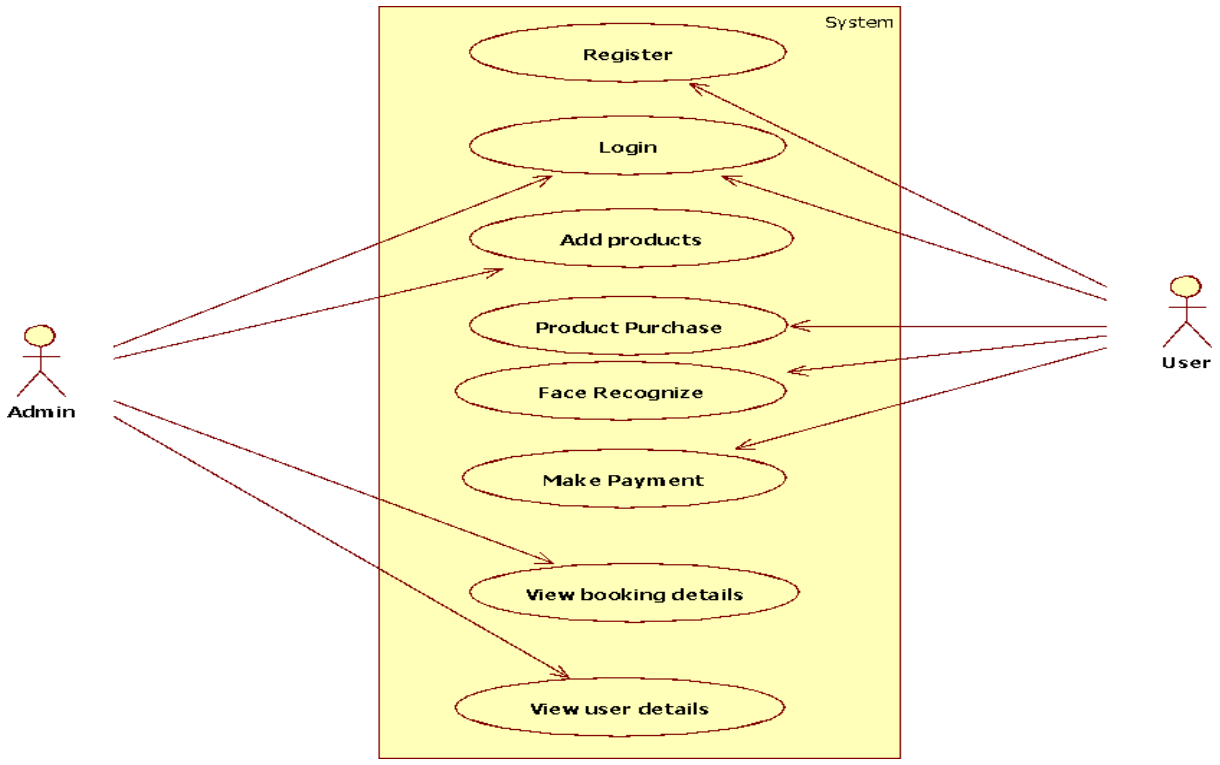


Figure 3.3.4 Usecase Diagram

CLASS DIAGRAM

A class diagram in the Unified Modeling Language is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations, and the relationships among objects.The Purpose of Class Diagrams is a business Analysts can use class diagrams to model systems from a business perspective.

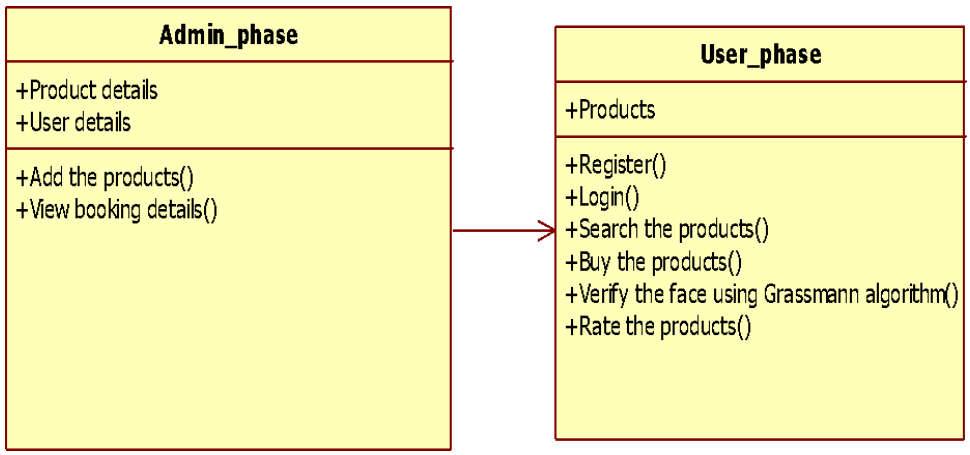


Figure 3.5 Class Diagram

SEQUENCE DIAGRAM

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence Diagrams are time focused and they show the order of the interaction visually by using the vertical axis of the diagram to represent time, what messages are sent and when. Sequence Diagrams capture high-level interactions between users of the system and the system, between the system and other systems, or between subsystems.

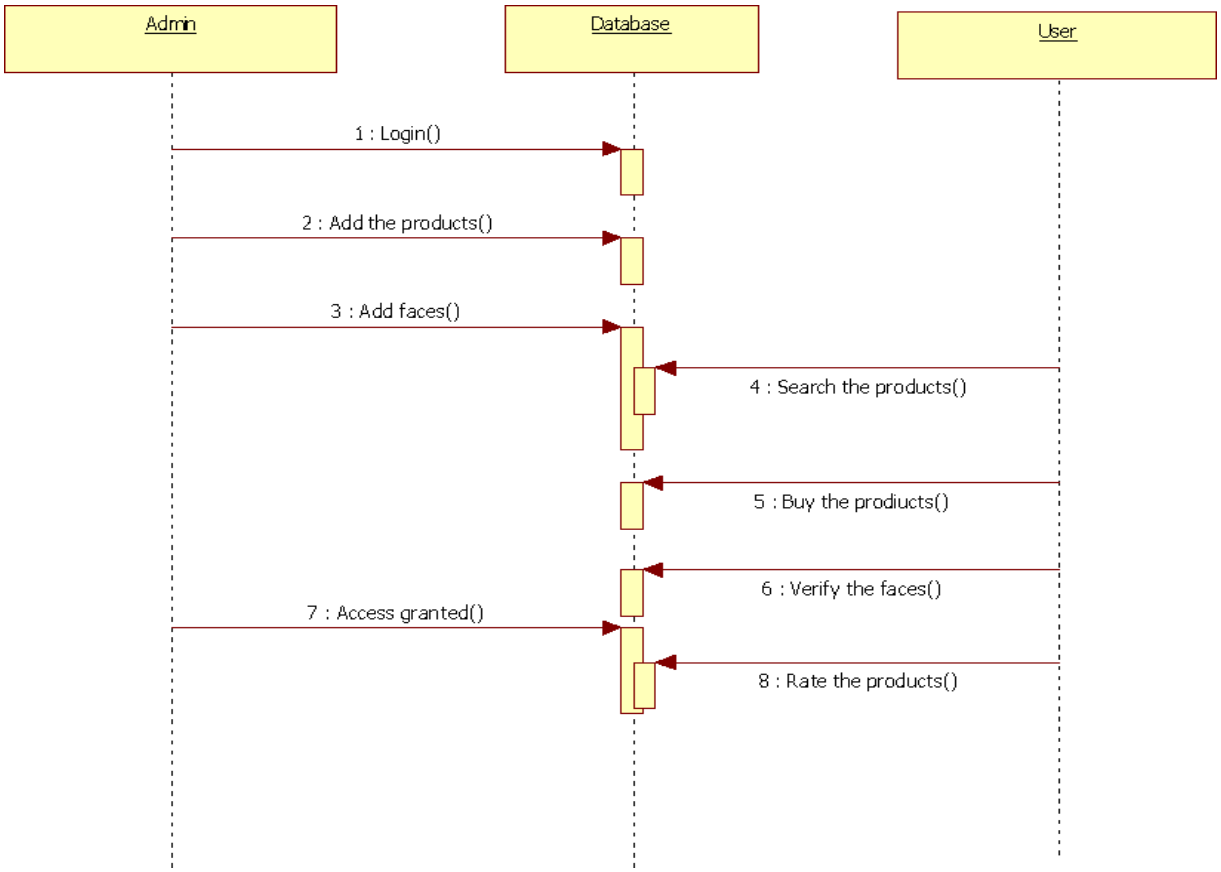


Figure 3.3.6 Sequence Diagram

ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. Activity diagram is a behavioral diagram in UML diagram to describe dynamic aspects of the system. Activity diagram is essentially an advanced version of flowchart that models the flow from one activity to another activity. Activity Diagrams describe how activities are coordinated to provide a service which can be at different levels of abstraction. The basic purpose of activity diagrams is similar to the other four diagrams. It captures the dynamic behavior of the system.

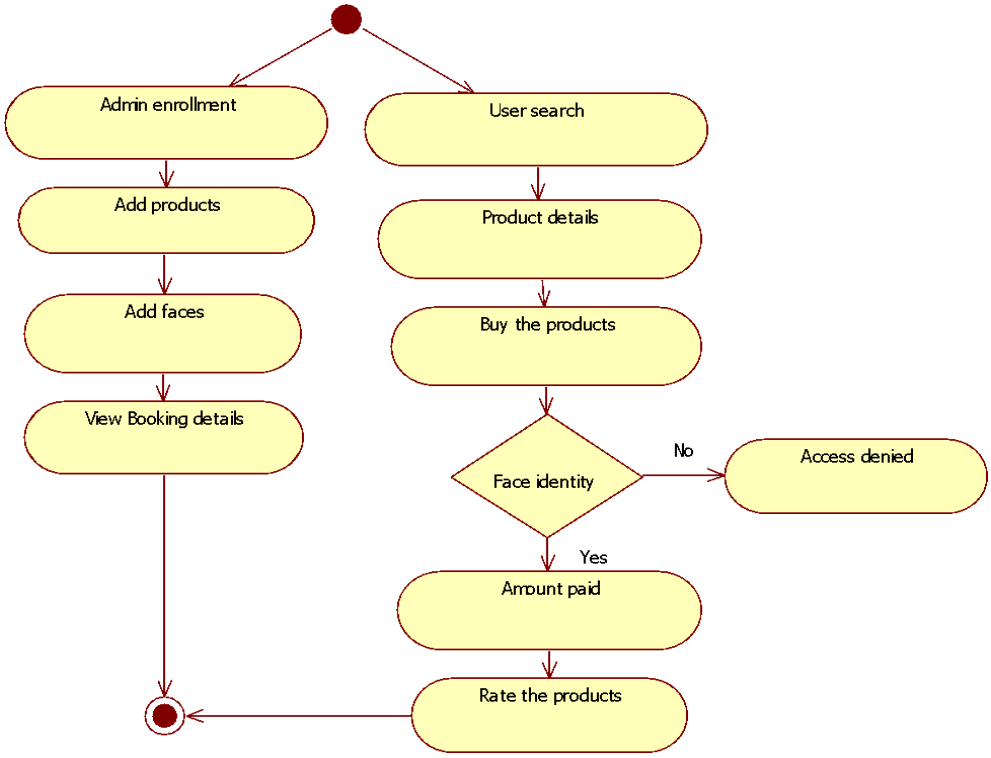


Figure 3.7 Activity Diagram

3.4 PROGRAM DESIGN

METHODOLOGY

The Grassmannian algorithm deals with the Grassmann manifold, which is a space of all possible linear subspaces of a given space. In face recognition, some methods use subspace- based techniques, where faces are represented as points in a high-dimensional space, often with Principal Component Analysis (PCA) or similar techniques. During face recognition, the algorithm aims to find the subspace that best represents the faces in the dataset. This subspace is essentially a low-dimensional representation of the high-dimensional face images. Now, if we want to connect this to credit card fraud detection: Just like faces are represented in a lower- dimensional subspace, credit card transactions can be represented in a lower-dimensional space of features. Anomalies in this space could represent potentially fraudulent transactions. The Grassmannian algorithm, or its related concepts, could potentially be used to find the best subspace representation of normal transaction behavior.

The Grassmann manifold is a type of Grassmann manifold. The set of m-dimensional linear subspaces of the R D is known as G(m, D). The G(m, D) is a compact Riemannian manifold with m(Dm) dimensions.

An orthonormal matrix Y of size D by m can be used to represent an element of G(m, D), with Y = Im, where Im is the m by m identity matrix. For instance, Y may represent the m basis vectors of a set of R D photographs. However, the matrices Y1 and Y2 are considered the same if and only if span(Y1) = span(Y2), where span(Y) signifies the subspace spanned by the column vectors of Y. In other words, if and only if Y1R1 = Y2R2 for some R1, R2 O, span(Y1) = span(Y2) (m). With this understanding, we will frequently use the notation Y to refer to its equivalence class span(Y), and Y1 = Y2 to refer to span(Y1) = span(Y2).

The length of the shortest geodesic connecting two points on the Grassmann manifold is the Riemannian distance between two subspaces. However, utilising the principal angles to define the distances is a more intuitive and computationally efficient method.

Input: A set of P points on manifold { } $P \in (d, D)$ Output: Karcher meanμK 1. Set an initial estimate of Karcher mean $\mu K = Xi$by randomly picking one point in $Xi\}$ 2. Compute the average tangent vector A = 1 $\sum P$ ⬚ log ( ) i=1 P μK i i= 1 3. If $\|A\| < \varepsilon$ then return μK stop, else go to Step 4 4. Move μK in average tangent direction $\mu K = e(\alpha A)$, where$\alpha > 0$ is a xxx 35 parameter of step size. Go to Step 2, until μK meets the termination conditions.

Face representation: Next, the extracted facial features are represented as points in a high- dimensional space. This space is often referred to as a feature space or a face space.

Grassmann manifold: The Grassmann manifold is a mathematical space that represents all possible subspaces of a fixed dimension in a high-dimensional space. The Grassmann algorithm uses this manifold to compare the subspaces that represent the facial features of different faces.

Subspace projection: Each face is represented as a subspace in the feature space. The Grassmann algorithm then projects these subspaces onto the Grassmann manifold to create a set of points that can be compared.

Distance computation: Finally, the distance between the subspaces is computed using a distance metric such as the Grassmann distance. The distance metric takes into account t geometry of the Grassmann manifold and provides a measure of how similar or dissimilar the subspaces.

CHAPTER 4

PROPOSED SYSTEM

The proposed system is developed after a detailed study about the requirements requested by the user. Proposed system is a computerized one, where all the limitations of manual system are compensated. Product details of online shopping system with credit card transaction based on face recognition technology have simplified the working information and make a user friendly environment, where the user is provided with much flexibility to manage effectively. It helps the retailer to generate desirable reports more quickly and also to produce better results.

In the proposed system, we are using face recognition using web application to provide secure transaction authenticity of credit card holder for online shopping. For recognition of face images, here implement Grassmann Learning approach. Grassmann learning is a dimensionality reduction algorithm where subspaces are mapped as points onto a smooth and curved surface where distances between subspaces are geodesic.

The main advantage of Grassmann learning over traditional manifold learning methods is that high dimensional feature representations may not typically lie on a Euclidean space. Grassmann learning maps subspaces onto points based on orthogonal constraints, promoting high between class discrimination by their geometrical structuring, and accounting for missing data through subspace spanning. Grassmann learning involves embedding high dimensional subspaces and kernelling the embedding onto a projection space where distance computations can be effectively performed.

In this project the user can buy a product through this website, after buying the products the user can pay the amount using credit card transaction with face

detection. So face detection verifies user face by capturing it using camera, after successful face detection method the user can pay the purchased amount.

ADVANTAGES OF PROPOSED SYSTEM

- Face authentication provides complete security of the proposed method in real time fraud analysis.
- Overcome the guessing attacks and dictionary attacks.
- No need to implement additional sensors.
- SMS alert to know about transactions details up to date.

4.1 ARCHITECTURE DIAGRAM

System architecture involves the high-level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability. Software architecture must describe its group of components, their connections, interactions among them and deployment configuration of all component

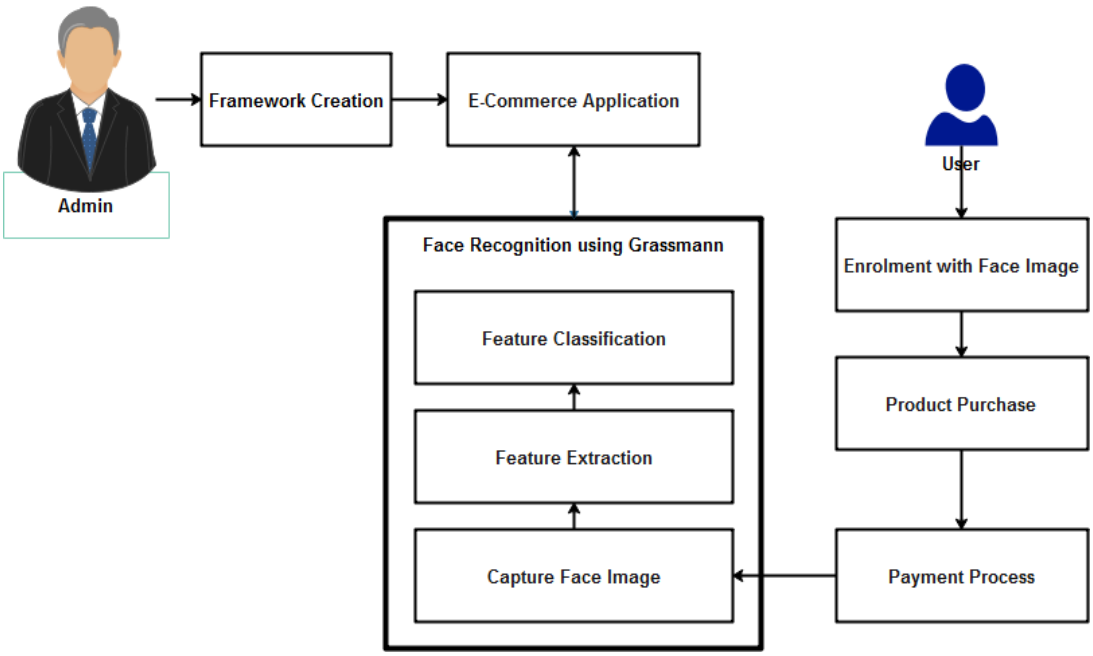


Fig 4.1.1 Architecture diagram

4.2 MODULES

- Framework Creation
- Purchase Product
- Payment Using Face Recognition
- Face Classification
- Payment Process

4.3 IMPLEMENTATION OF MODULES

4.3.1. FRAMEWORK CREATION

Framework creation is the process of developing E-commerce application with proposed facilities. In this application admin can add the product details like product id, name, type, amount, quantity and so on. Then user can create their account by providing required information to the system. The registration form details are like user name, email, gender, mobile number, address, and credit card details etc. Here user's face image captured through web cameras and registered in database for further verification. These details are stored in the database. And then can getting to the username and password in the system.

4.3.2 PURCHASE PRODUCT

In this module, user can login in E-Commerce application and search product for purchasing. The user can view the product details like product name, type, amount, description etc. After viewing all products, the user can select product based on their need. The user's purchase details are sent to the admin.

4.3.3 PAYMENT USING FACE RECOGNITION

In proposed E-Commerce application user can make payment securely with the help of face recognition approach. This module contains user's card details like name, card no, amount etc. After successfully entered the card details the system,

user's face image was captured with the help of web camera. Then the captured face image compared with card holder account database. If the user face image is matched with database, the user payment is transferred. Otherwise, the user payment is not transferred.

4.3.4 FACE CLASSIFICATION

Face classification is the process of extraction facial features and compared with database for user verification. Facial highlights such as nose part, eye parts and lip part are extracted as feature values. These qualities are put away is as grid. The framework can be shaped by utilizing Grassmann manifold learning computation. The feature data of particular facial image helps its application as a biometric identifier for individual acknowledgment. Face acknowledgment frameworks set up the nearness of an approved individual instead of simply checking whether a legitimate (ID) or key is being utilized or whether the client knows the secret individual ID numbers (Pins) or passwords. At the point when the main two coordinated countenances are exceptionally like the verification of face image.

4.3.5 PAYMENT PROCESS

Once the face detection process is completely finished then the user can move on to the payment process. Here users can enter the amount that should be transferred. Then the amount transaction was completed in a highly secure manner. When the classification process fails to detect the face image or identify the fake user the system will automatically send e- mail notification to the customer as soon as the order is place.

CHAPTER 5

SYSTEM SPECIFICATION

5.1 HARDWARE REQUIREMENTS

- Processor : Intel Pentium 4
- RAM : 4 GB
- Hard disk : 160 GB
- Compact Disk : 650 Mb
- Keyboard : Standard keyboard
- Monitor : 15 inch color monitor

5.2 SOFTWARE REQUIREMENTS

- Operating System : Windows OS
- Front End : HTML , CSS, JAVASCRIPT
- Back End : Python
- Database : MySQL server
- Application : Web Application
- Tool : VS Code

5.3 FRONT END

HTML

HTML is a markup language for describing web documents (web pages).

- Hyper is the opposite of linear. It used to be that computer programs had

to move in a linear fashion. This before this, this before this, and so on. HTML does not hold to that pattern and allows the person viewing the World Wide Web page to go anywhere, anytime they want.

- Text is what you will use. Real, honest to goodness English letters.
- Mark up is what you will do. You will write in plain English and then mark up what you wrote. More to come on that in the next Primer.
- Language because they needed something that started with " L " to finish HTML and Hypertext Markup Louie didn't flow correctly. Because it's a language, really but the language is plain English.

HTML remains for Hyper Text Markup Language. It is a basic content designing dialect used to make hypertext records. It is a stage free dialect not at all like most other programming dialect. HTML is impartial and can be utilized on numerous stage or desktop. It is this component of HTML that makes it mainstream as standard on the WWW.

CSS

Cascading Style Sheets (CSS) is a style sheet language used for specifying the presentation and styling of a document written in a markup language such as HTML or XML (including XML dialects such as SVG, MathML or XHTML). CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript. CSS is designed to enable the separation of content and presentation, including layout, colors, and fonts. This separation can improve content accessibility;[further explanation needed] provide more flexibility and control in the specification of presentation characteristics; enable multiple web pages to share formatting by specifying the relevant CSS in a separate .css file, which reduces complexity and repetition in the structural content; and enable the .css file to be cached to improve the page load speed between the pages that share the file and its formatting.Separation of formatting and content

also makes it feasible to present the same markup page in different styles for different rendering methods, such as on-screen, in print, by voice (via speech-based browser or screen reader), and on Braille-based tactile devices. CSS also has rules for alternate formatting if the content is accessed on a mobile device.

The name cascading comes from the specified priority scheme to determine which declaration applies if more than one declaration of a property match a particular element. This cascading priority scheme is predictable. The CSS specifications are maintained by the World Wide Web Consortium (W3C). Internet media type (MIME type) text/css is registered for use with CSS by RFC 2318 (March 1998). The W3C operates a free CSS validation service for CSS documents.

In addition to HTML, other markup languages support the use of CSS including XHTML, plain XML, SVG, and XUL. CSS is also used in the GTK widget toolkit.

JAVASCRIPT

JavaScript is an open-source programming language designed for creating web-centric applications. It is lightweight and interpreted which makes it much faster than other languages and is integrated with HTML making it easier to implement in web applications.

In this Introduction to JavaScript article, you will learn all about JavaScript, the backbone of web development, and understand what exactly this language is and why and how this language is used across various fields. JavaScript is critical for web development, and if you've ever thought about choosing that career path, you'd surely have come across this language. And probably, that's why you are here in the first place. JavaScript is an essential programming language, almost compulsory to learn for students or software developers that are gravitated towards

web development. Wondering why? Here's the answer: Javascript is the most popular programming language in the world and that makes it a default choice for web development. There are many frameworks available which you can use to create web applications once you have learned JavaScript. JavaScript offers lots of flexibility. You can create stunning and fast web applications with tons of customizations to provide users with the most relevant graphical user interface

5.4 BACK END: PYTHON

Python is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. It was created by Guido van Rossum during 1985- 1990. Like Perl, Python source code is also available under the GNU General Public License (GPL). This tutorial gives enough understanding on Python programming language.

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages. Python is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain. Python is currently the most widely used multi-purpose, high-level programming language. Python allows programming in Object-Oriented and Procedural paradigms. Python programs generally are smaller than other programming languages like Java.

Programmers have to type relatively less and indentation requirement of the language, makes them readable all the time. Python language is being used by

almost all tech-giant companies like – Google, Amazon, Facebook, Instagram, Dropbox, Uber… etc. The biggest strength of Python is huge collection of standard libraries which can be used for the following:

- Machine Learning
- GUI Applications (like Kivy, Tkinter, PyQt etc.)
- Web frameworks like Django (used by YouTube, Instagram, Dropbox)
- Image processing (like OpenCV, Pillow)
- Web scraping (like Scrapy, BeautifulSoup, Selenium)
- Test frameworks
- Multimedia
- Scientific computing
- Text processing and many more.

Pillow

Pillow is the friendly PIL fork by Alex Clark and Contributors. PIL is the Python Imaging Library by Fredrik Lundh and Contributors. Python pillow library is used to image class within it to show the image. The image modules that belong to the pillow package have a few inbuilt functions such as load images or create new images, etc.

OpenCV

OpenCV is an open-source library for the computer vision. It provides the facility to the machine to recognize the faces or objects. In OpenCV, the CV is an abbreviation form of a computer vision, which is defined as a field of study that helps computers to understand the content of the digital images such as photographs and videos.

Tensor Flow

TensorFlow is an end-to-end open-source platform for machine learning. It has a comprehensive, flexible ecosystem of tools, libraries, and community resources that lets researchers push the state-of-the-art in ML, and gives developers the ability to easily build and deploy ML-powered applications.

Pandas

Pandas is a fast, powerful, flexible and easy to use open source data analysis and manipulation tool, built on top of the Python programming language. pandas is a Python package that provides fast, flexible, and expressive data structures designed to make working with "relational" or "labeled" data both easy and intuitive. It aims to be the fundamental high-level building block for doing practical, real world data analysis in Python. Pandas is mainly used for data analysis and associated manipulation of tabular data in Data frames. Pandas allows importing data from various file formats such as comma- separated values, JSON, Parquet, SQL database tables or queries, and Microsoft Excel. Pandas allows various data manipulation operations such as merging, reshaping, selecting, as well as data cleaning, and data wrangling features.

The development of pandas introduced into Python many comparable features of working with Data frames that were established in the R programming language. The panda's library is built upon another library NumPy, which is oriented to efficiently working with arrays instead of the features of working on Data frames.

NumPy

NumPy, which stands for Numerical Python, is a library consisting of multidimensional array objects and a collection of routines for processing those arrays. Using NumPy, mathematical and logical operations on arrays can be performed. NumPy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays.

Matplotlib

Matplotlib is a comprehensive library for creating static, animated, and interactive visualizations in Python. Matplotlib makes easy things easy and hard things possible. Matplotlib is a plotting library for the Python programming language and its numerical mathematics extension NumPy. It provides an object-oriented API for embedding plots into applications using general-purpose GUI toolkits like Tkinter, wxPython, Qt, or GTK.

5.5 DATABASE: MySQL

MySQL tutorial provides basic and advanced concepts of MySQL. Our MySQL tutorial is designed for beginners and professionals. MySQL is a relational database management system based on the Structured Query Language, which is the popular language for accessing and managing the records in the database. MySQL is open-source and free software under the GNU license. It is supported by Oracle Company. MySQL database that provides for how to manage database and to manipulate data with the help of various SQL queries. These queries are: insert records, update records, delete records, select records, create tables, drop tables, etc. There are also given MySQL interview questions to help you better understand the MySQL database.

MySQL is currently the most popular database management system software used for managing the relational database.

It is open-source database software, which is supported by Oracle Company. It is fast, scalable and easy to use database management system in comparison with Microsoft SQL Server and Oracle Database. It is commonly used in conjunction with PHP scripts for creating powerful and dynamic server- side or web-based enterprise applications. It is developed, marketed, and supported by MySQL AB, a Swedish company, and written in C programming language and C++ programming language. The official pronunciation of MySQL is not the My Sequel; it is My Ess Que Ell. However, you can pronounce it in your way. Many small and big companies use MySQL. MySQL supports many Operating Systems like Windows, Linux, MacOS, etc. with C, C++, and Java languages.

RDBMS Terminology

Before we proceed to explain the MySQL database system, let us revise a few definitions related to the database.

- Database − A database is a collection of tables, with related data.
- Table − A table is a matrix with data. A table in a database looks like a simple spreadsheet.
- Column − One column (data element) contains data of one and the same kind, for example the column postcode.
- Row − A row (= tuple, entry or record) is a group of related data, for

example the data of one subscription.

MySQL Database

MySQL is a fast, easy-to-use RDBMS being used for many small and big businesses. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company. MySQL is becoming so popular because of many good reasons −

- MySQL is released under an open-source license. So you have nothing to pay to use it.
- MySQL is a very powerful program in its own right. It handles a large subset of the functionality of the most expensive and powerful database packages.
- MySQL uses a standard form of the well-known SQL data language.
- MySQL works on many operating systems and with many languages including PHP, PERL, C, C++, JAVA, etc.
- MySQL is customizable. The open-source GPL license allows programmers to modify the MySQL software to fit their own specific environments.

CHAPTER 6

CONCLUSION AND FUTURE ENHANCEMENT

6.1 CONCLUSION

This project entitled “CREDIT CARD FRAUD DETECTION” has been developed to satisfy all the proposed requirements. The process of recording details about online shopping is simpler and easier. The system reduces the possibility of errors to a great extent and maintains the data in an efficient manner. User friendliness is the unique feature of this system. The system generates the reports as and when required. The system is highly interactive and flexible for further enhancement. The coding is done in a simplified and easy to understand manner so that other teams trying to enhance the project can do so without facing much difficulty. The documentation will also assist in the process as it has also been carried out in a simplified and concise way.

6.2 FUTURE ENHANCEMENT

While face recognition technology can be an effective way to prevent fraud, it's not fool proof. Future work could focus on developing additional security measures, such as multi-factor authentication or biometric sensors, to further enhance the security of credit card transactions. Also focus on expanding the usability of this technology so that it's available to more consumers and businesses.

APPENDICES

A.1 SAMPLE SOURCE CODE

```
from flask import Flask, render_template, flash, request, session
import mysql.connector

from werkzeug.utils import secure_filename
from flask import Flask, render_template, request, jsonify import datetime
import re
import sys import socket
hostname = socket.gethostname() IPAddr = socket.gethostbyname(hostname) app
= Flask(_name_) app.config.from_object(_name_)
app.config['SECRET_KEY'] = '7d441f27d441f27567d441f2b6176a'
@app.route("/ ") def homepage():
return render_template('index.html')
@app.route("/AdminLog in") def AdminLogin():

return render_template('AdminLogin.html') @app.route("/NewUser")
def NewUser():

import LiveRecognition  as liv del sys.modules["LiveRecognition"] return
render_template('NewUser.html')
@app.route("/UserLogin ") def UserLogin():
return render_template('UserLogin.html')
@app.route("/viewproduct", methods=['GET', 'POST']) def viewproduct():
# searc = request.args.get('subcat')

searc = request.form['subcat']
conn1 = mysql.connector.connect(user='root', password='', host='localhost',
 database='2creditcardpy')
cur1 = conn1.cursor() cur1.execute(
   "SELECT * from protb where SubCategory like '%" + searc + "%' ") data =
cur1.fetchall()
data1 = "

return render_template('ViewProduct.html', data=data, data1=data1)
@app.route("/AdminHo me") def AdminHome():
   conn1 = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')
cur1 = conn1.cursor() cur1.execute("SELECT * FROM reg tb ")
data = cur1.fetchall()

# return 'file register successfully'

# return render_template('order.html', data=data)
```

```
return render_template('AdminHome.html', data=data)
@app.route("/NewProdu ct") def NewProduct():
    conn1 = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')
cur1 = conn1.cursor()
cur1.execute("SELECT DISTINCT ProductType FROM protb ") data =
cur1.fetchall()
return render_template('NewProduct.html', data=data)
@app.route("/Search ") def Search():
    conn1 = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')
cur1 = conn1.cursor() cur1.execute("SELECT * FROM protb ") data = cur1.fetchall()
return render_template('ViewProduct.html', data=data)
@app.route("/ProductInf o") def ProductInfo():
    conn1 = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')
cur1 = conn1.cursor() cur1.execute("SELECT * FROM protb ") data = cur1.fetchall()
return render_template('ProductInfo.html', data=data)
@app.route("/SalesInfo ") def SalesInfo():
return render_template('SalesInfo.html')
@app.route("/FeedBackInf o") def FeedBackInfo():
return render_template('FeedBackInfo.html')
@app.route("/RNewUser", methods=['GET', 'POST']) def RNewUser():
if request.method == 'POST': name1 = request.form['name'] gender1 =
request.form['gender'] Age
= request.form['age'] email = request.form['email'] address = request.form['address']
pnumber = request.form['phone'] uname = request.form['uname'] password =
request.form['psw']
      conn = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')
cursor = conn.cursor() cursor.execute(
"INSERT INTO regtb VALUES ('" + name1 + "','" + gender1 + "','" + Age + "','" +
email + "','" + pnumber + "','" + address + "','" + uname + "','" + password + "')")
conn.commit()
conn.close()
# return 'file register successfully'
return render_template('userlogin.html')
@app.route("/RNewProduct", methods=['GET', 'POST']) def RNewProduct():
if request.method == 'POST':
file = request.files['fileupload'] file.save("static/upload/" + file.filename)
ProductId = request.form['pid'] Gender = request.form['gender'] Category =
request.form['cat'] SubCategory = request.form['subcat'] ProductType =
request.form['ptype'] Colour =
```

```
request.form['color']

Usage = request.form['usage'] ProductTitle = request.form['ptitle']
Image = file.filename

ImageURL = "static/upload/" + file.filename
      conn = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')

cursor = conn.cursor() cursor.execute(
        "INSERT INTO protb VALUES ('" + ProductId + "','" + Gender + "','" +
Category + "','" + SubCategory + "','" + ProductType + "','" + Colour + "','" +
   Usage + "','" + ProductTitle + "','" + Image + "','" + ImageURL + "')")
conn.commit()
conn.close()

# return 'file register successfully'
return render_template('NewProduct.html')
@app.route("/NewCar d") def NewCard():
   conn1 = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')
cur1 = conn1.cursor()
cur1.execute("SELECT * FROM cardtb where UserName="'+ session['uname'] +"'  ")
data = cur1.fetchall()
return render_template('NewCardInfo.html',data=data)


@app.route("/RNewcard", methods=['GET', 'POST']) def RNewcard():
if request.method == 'POST': cno =
request.form['cno'] ctype

= request.form['ctype'] exm = request.form['exm'] exy
= request.form['exy'] cnvo = request.form['cnvo'] pin
= request.form['pin'] uname = session['uname']
      conn = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')
cursor = conn.cursor() cursor.execute(
"INSERT INTO cardtb VALUES ('" + uname + "','" + cno + "','" + ctype + "','" +

exm + "','" + exy + "','" + cnvo +

"','" + pin + "','Active')")

conn.commit() conn.close()
# return 'file register successfully'

return render_template('NewCardInfo.html')
```

```
@app.route("/userlogin", methods=['GET', 'POST']) def userlogin():
error = None

if request.method == 'POST': username = request.form['uname'] password =
request.form['password']
session['uname'] = request.form['uname'] session['count'] = 0
      conn = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')
cursor = conn.cursor()

      cursor.execute("SELECT * from regtb where UserName='" + username + "' and
password='" + password + "'")
data = cursor.fetchone() if data is None:
data1 = 'Username or Password is wrong'

return render_template('goback.html', data=data1)
else:

         conn1 = mysql.connector.connect(user='root', password='', host='localhost',
database='2creditcardpy')


cur1 = conn1.cursor()

cur1.execute("SELECT * FROM regtb where username='" + session['uname'] + "' ")
data = cur1.fetchall()
# return 'file register successfully'

# return render_template('order.html', data=data)
return render_template('UserHome.html', data=data)
```

A.2 SAMPLE SCREENSHOTS

Figure A.2.1 Home Page

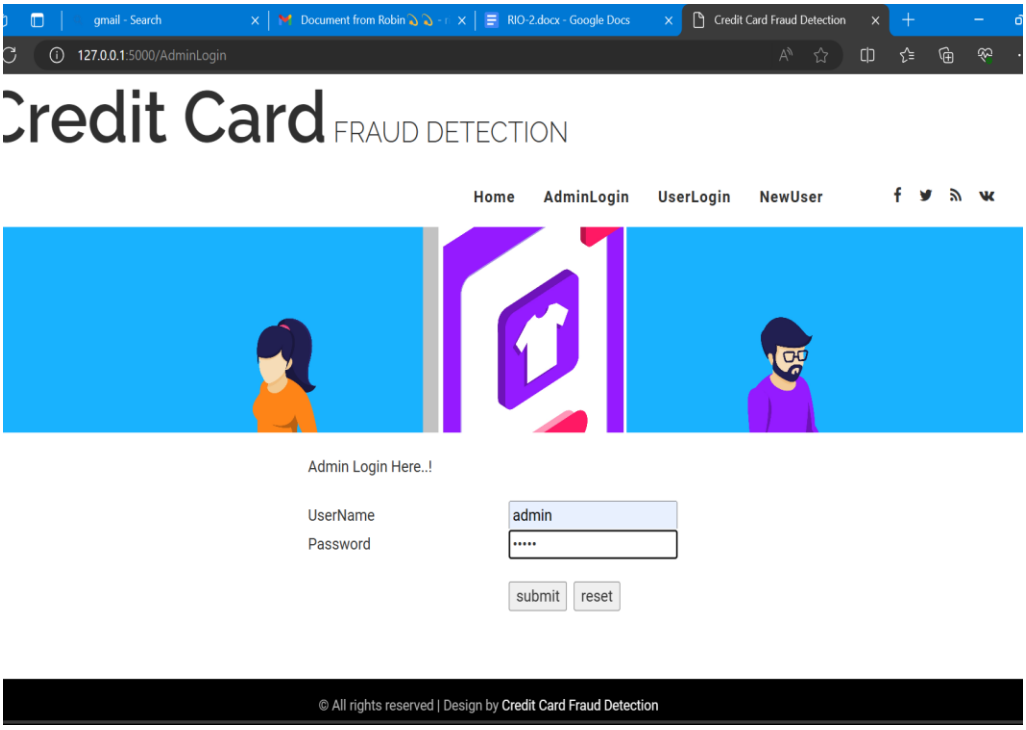


Figure A.2.2 Admin Login Page

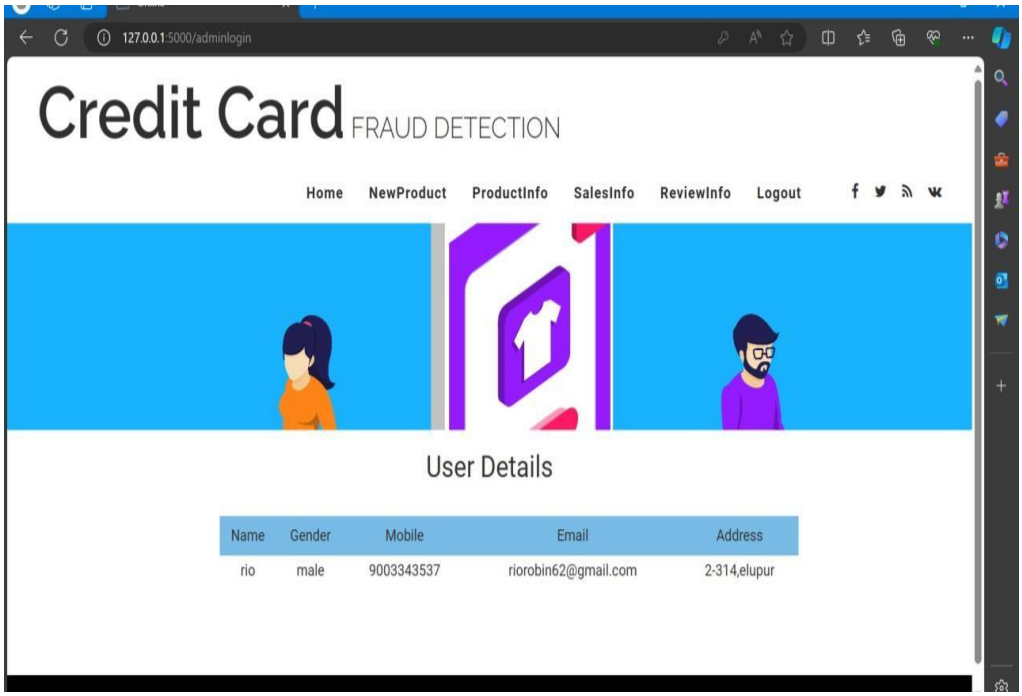


Figure A.2.3 User Details Page

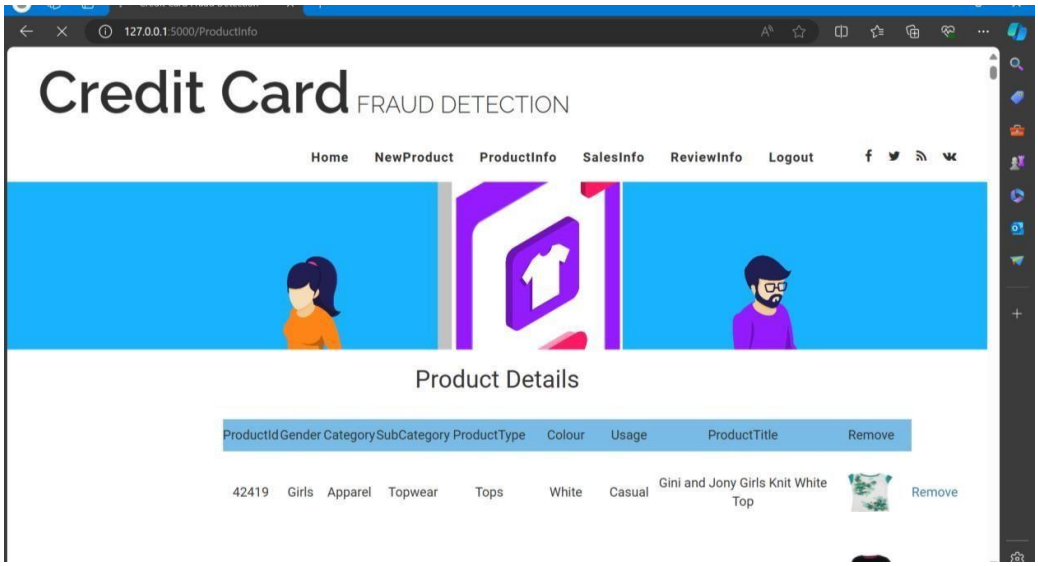
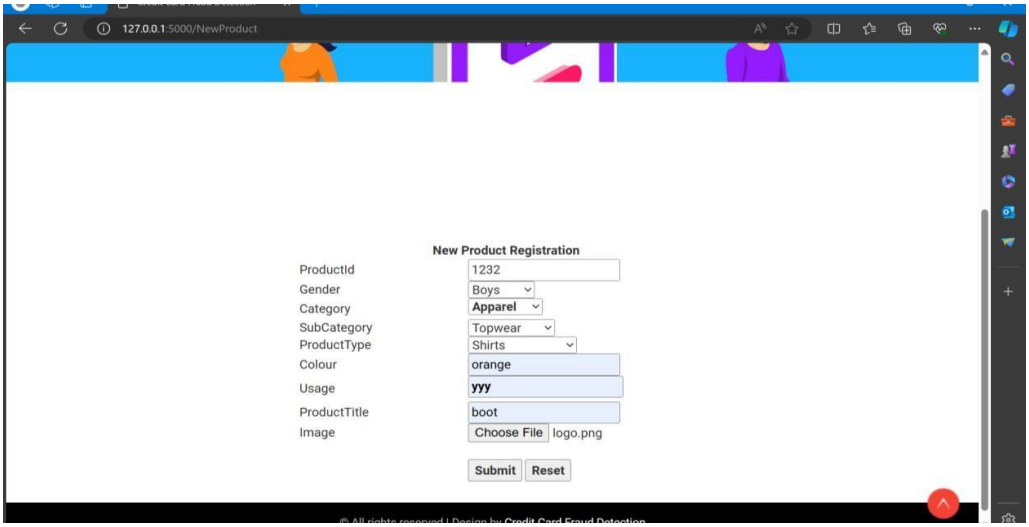
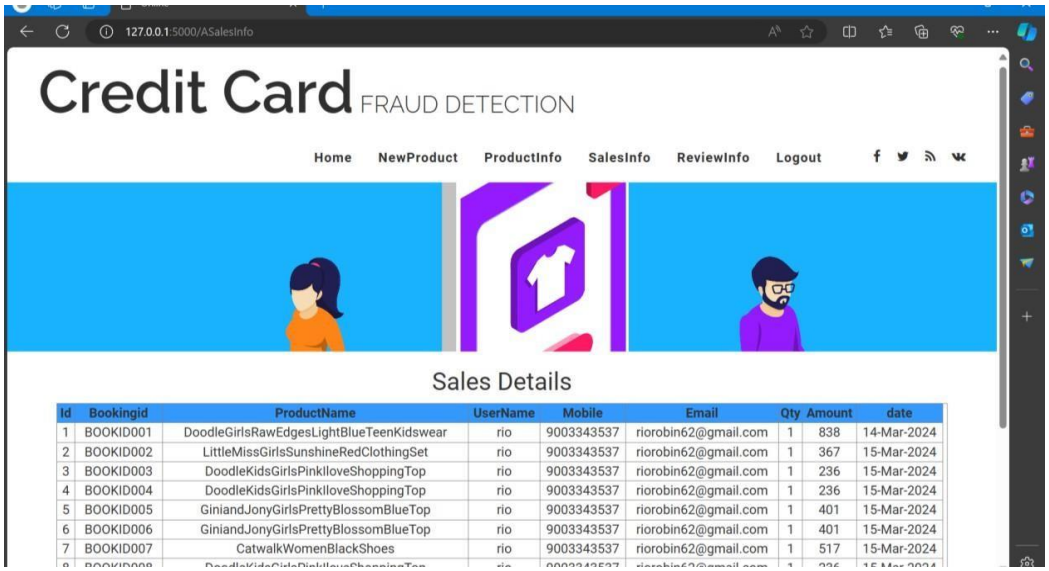


Figure A.2.4 New product Registration Page

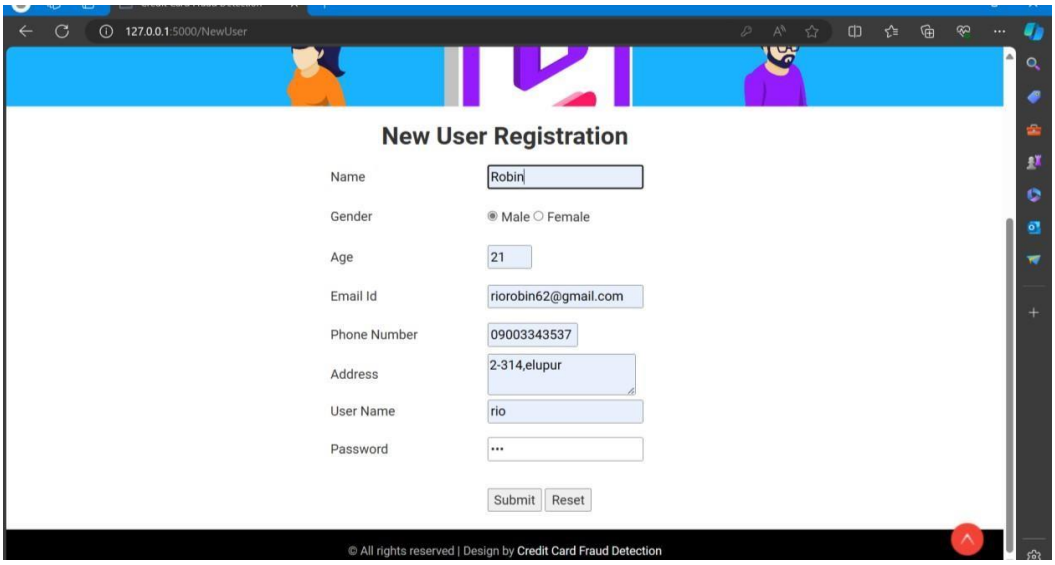


A.2.5 product Details

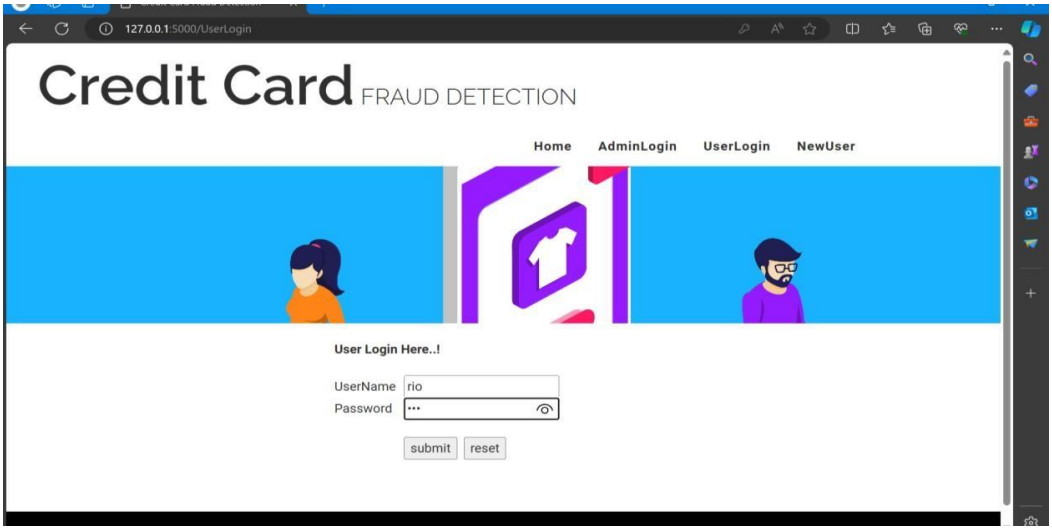


Id	Bookingid	ProductName	UserName	Mobile	Email	Qty	Amount	date
1	BOOKID001	DoodleGirlsRawEdgesLightBlueTeenKidswear	rio	9003343537	riorobin62@gmail.com	1	838	14-Mar-2024
2	BOOKID002	LittleMissGirlsSunshineRedClothingSet	rio	9003343537	riorobin62@gmail.com	1	367	15-Mar-2024
3	BOOKID003	DoodleKidsGirlsPinkIloveShoppingTop	rio	9003343537	riorobin62@gmail.com	1	236	15-Mar-2024
4	BOOKID004	DoodleKidsGirlsPinkIloveShoppingTop	rio	9003343537	riorobin62@gmail.com	1	236	15-Mar-2024
5	BOOKID005	GiniandJonyGirlsPrettyBlossomBlueTop	rio	9003343537	riorobin62@gmail.com	1	401	15-Mar-2024
6	BOOKID006	GiniandJonyGirlsPrettyBlossomBlueTop	rio	9003343537	riorobin62@gmail.com	1	401	15-Mar-2024
7	BOOKID007	CatwalkWomenBlackShoes	rio	9003343537	riorobin62@gmail.com	1	517	15-Mar-2024

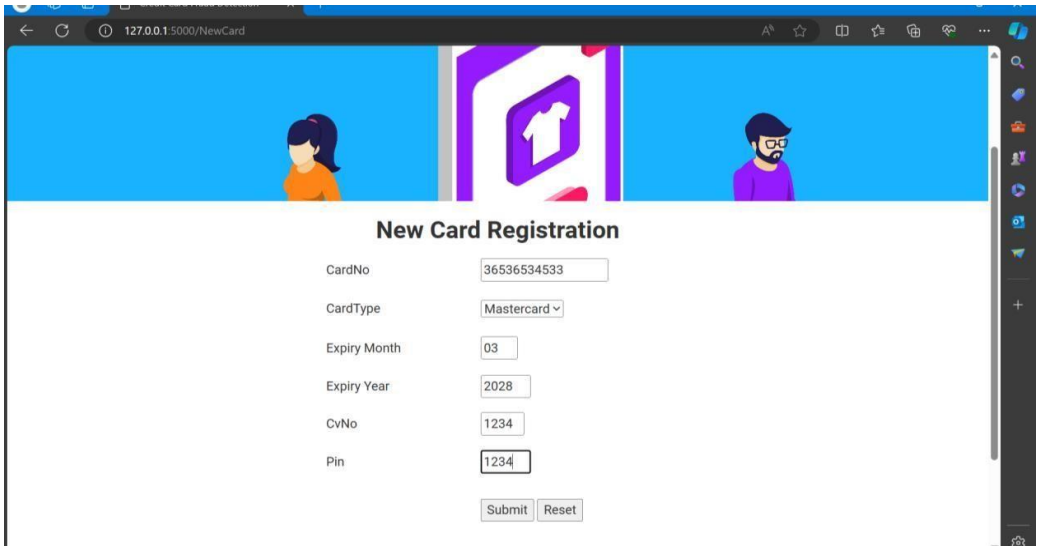
A.2.6 Sales Details



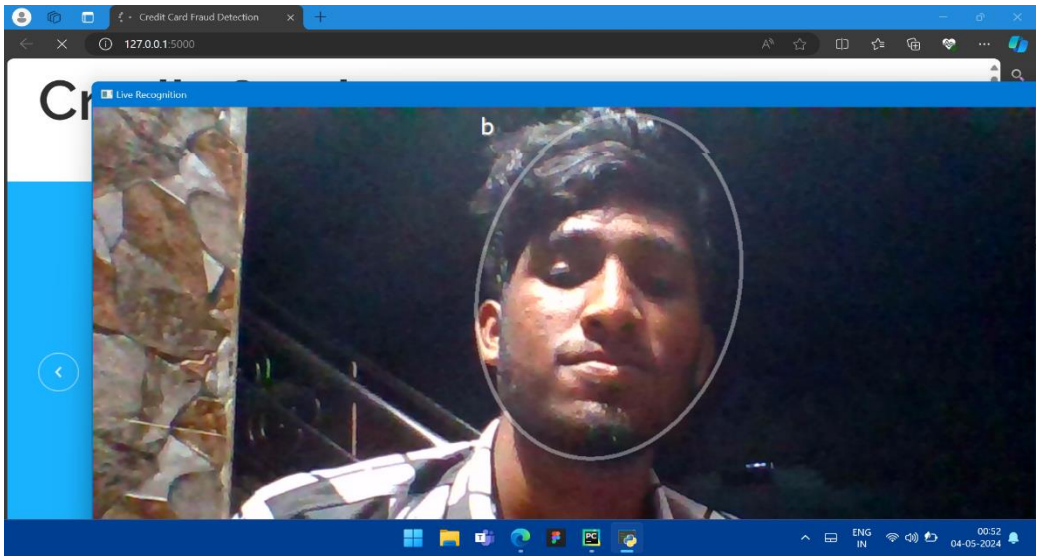
A.2.7 New user Registration Page



A.2.8 User login Page



A.2.9 New Card Registration Page



A.2.10 Face Recognition

REFERENCES

[1] Sahu, Aanchal, G. M. Harshvardhan, and Mahendra Kumar Gourisaria. "A dual approach for credit card fraud detection using neural network and data mining techniques." In 2020 IEEE 17th India council international conference (INDICON), pp. 1-7. IEEE, 2020.

[2] Panda, Agyan, Bharath Yadlapalli, and Zhi Zhou. "Credit card fraud detection through machine learning algorithm." Big Data and Computing Visions 1, no. 3 (2021): 140-145.

[3] Kumar, Sheo, Vinit Kumar Gunjan, Mohd Dilshad Ansari, and Rashmi Pathak. "Credit Card Fraud Detection Using Support Vector Machine." In Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications: ICMISC 2021, pp. 27-37. Springer Singapore, 2022.

[4] Vinaya, D. S., Satish B. Basapur, Vanishree Abhay, and Neetha Natesh. "Credit Card Fraud Detection Systems (CCFDS) using Machine Learning (Apache Spark)." (2020).

[5] Lucas, Yvan, and Johannes Jurgovsky. "Credit card fraud detection using machine learning: A survey." arXiv preprint arXiv:2010.06479 (2020).

[6] Singh, Gurpreet, Divyanshi Kaushik, Hritik Handa, Gagandeep Kaur, Sunil Kumar Chawla, and A. Ahmed. "BioPay: a secure payment gateway through biometrics." Journal of Cybersecurity and Information Management 7, no. 2 (2021).

[7] Aziz, Amir, and Hamid Ghous. "Fraudulent Transactions Detection in Credit Card by using Data Mining Methods: A Review." INTERNATIONAL JOURNAL OF SCIENTIFIC PROGRESS AND RESEARCH (IJSPR) 79, no. 179 (2021).

[8] Shah, Ankit, and Akash Mehta. "Comparative Study of Machine Learning Based Classification Techniques for Credit Card Fraud Detection." In 2021 International Conference on Data Analytics for Business and Industry (ICDABI), pp. 53-59. IEEE, 2021.

[9] Muttipati, Appala Srinuvasu, Sangeeta Viswanadham, Radhika Senapathi, and KN Brahmaji Rao. "Recognizing credit card fraud using machine learning methods." Turkish Journal of Computer and Mathematics Education 12, no. 12 (2021): 3271-3278.

[10] Tiwari, Pooja, Simran Mehta, Nishtha Sakhuja, Jitendra Kumar, and Ashutosh Kumar Singh. "Credit card fraud detection using machine learning. study." arXiv preprint arXiv:2108.10005 (2021).

[11] Asosiasi Penyelenggara Jasa Internet Indonesia, " Magazine APJI (Asosiasi Penyelenggara Jasa Internet Indonesia)" (2019): 23 April 2018.

[12] Asosiasi Penyelenggara Jasa Internet Indonesia, "Mengawali integritas era digital 2019 - Magazine APJI (Asosiasi Penyelenggara Jasa Internet Indonesia)"(2019).

[13] Laudon, Kenneth C., and Carol Guercio Traver. Ecommerce: business, technology, society. 2016

[14] "Regulated AI calculations for Visa misrepresentation discovery: a correlation" a paper by S khatri and A. P. Agarwal

[15] Renjith, S. Detection of Fraudulent Sellers in Online Marketplaces using Support Vector Machine Approach. International Journal of Engineering Trends and Technology (2018).

[16] Roy, Abhimanyu, et al. "Deep learning detecting fraud in credit card transactions." 2018 Systems and Information Engineering Design Symposium (SIEDS). IEEE, 2018.

[17] Zhao, Jie, et al. "Extracting and reasoning about implicit behavioral evidences for detecting fraudulent online transactions in e-Commerce." Decision support

systems 86 (2016): 109-121

[18] Saputra, Adi & Suharjito, Suharjito. (2019). Fraud Detection using Machine Learning in e-Commerce. 10.14569/IJACSA.2019.0100943.

[19] Mahesh Poojari, Jobin Joseph, et al. “Credit Card Fraud Detection Using Random Forest Algorithm” International Journal of Trendy Research in Engineering and Technology Volume 5 Issue 3 June 2021.

[20] Subhash P, K R Sumana “Comparative Analysis of Credit Card Fraud Detection Using Machine Learning and Deep Learning Techniques” International Research Journal of Engineering and Technology (IRJET) Volume: 08 Issue: 08 | Aug 2021.

[21] Aditya Saini, Swarna Deep Sarkar “Credit Card Fraud Detection using Machine Learning and Data Science” International Journal of Engineering Research & Technology (IJERT) Vol. 8 Issue 09, September-2019.

[22] Das, Tamojit. (2019). Credit Card Fraud Detection Using Machine Learning With Python. 10.13140/RG.2.2.22851.35361/1.

[23] Emmanuel Ileberi, Yanxia Sun and Zenghui Wang “A machine learning based credit card fraud detection using the GA algorithm for feature selection” Ileberi et al. Journal of Big Data (2022) 9:24

[24] Heta Naik, Prashasti Kanikar “Credit card Fraud Detection based on Machine Learning Algorithms” International Journal of Computer Applications Volume 182 – No. 44, March 2019.

[25] Selvi P. Sankara Parvathy, M. Selvi “Credit Card Fraud Detection Using Deep Learning” Third International Conference on “Materials, Computing and Communication Technologies” Volume 9, Issue 12 - Published: June 20, 2022.