

Credit Card Fraud Detection System

**A PROJECT REPORT
for
Mini Project (KCA353)
Session (2023-24)**

Submitted by

**Rahul Singh Negi
2200290140120
Raj Srivastava
2200290140121**

**Submitted in partial fulfilment of the
Requirements for the Degree of**

MASTER OF COMPUTER APPLICATION

**Under the Supervision of
Mr. Prashant Aggarwal
Associate Professor**



Submitted to

**DEPARTMENT OF COMPUTER APPLICATIONS
KIET Group of Institutions, Ghaziabad
Uttar Pradesh-201206**

(MARCH 2024)

DECLARATION

I hereby declare that the work presented in report entitled “**Credit Card Fraud Detection System**” was carried out by me. I have not submitted the matter embodied in this report for the award of any other degree or diploma of any other University or Institute. I have given due credit to the original authors/sources for all the words, ideas, diagrams, graphics, computer programs, that are not my original contribution. I have used quotation marks to identify verbatim sentences and give credit to the original authors/sources. I affirm that no portion of my work is plagiarized, and the experiments and results reported in the report are not manipulated. In the event of a complaint of plagiarism and the manipulation of the experiments and results, I shall be fully responsible and answerable.

Name: Rahul Singh Negi

Roll No.: 2200290140120

Name: Raj Srivastava

Roll No.: 2200290140121

(Candidate Signature)

CERTIFICATE

Certified that **Rahul Singh Negi (2200290140120), Raj Srivastava (2200290140121)** has carried out the research work presented in this thesis entitled **“Credit Card Fraud Detection System”** for the award of **Master of Computer Application** from Dr. APJ Abdul Kalam Technical University, Lucknow under my/our (print only that is applicable) supervision. The thesis embodies results of original work, and studies are carried out by the student himself/herself (print only that is applicable) and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Date:

Rahul Singh Negi (2200290140120)

Raj Srivastava (2200290140121)

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date:

Mr. Prashant Aggarwal
Associate Professor
Department of Computer Applications
KIET Group of Institutions, Ghaziabad

Dr. Arun Tripathi
Head
Department of Computer Applications
KIET Group of Institutions, Ghaziabad

Credit Card Fraud Detection System

Raj Srivastava
Rahul Singh Negi

ABSTRACT

As the world is rapidly moving towards digitization and money transactions are becoming cashless, the use of credit cards has rapidly increased. The fraud activities associated with it have also been increasing which leads to a huge loss to the financial institutions. Therefore, we need to analyze and detect the fraudulent transaction from the non-fraudulent ones.

In this we present a comprehensive review of various methods used to detect credit card frauds. Here we implement different machine learning algorithms on an imbalanced dataset such as logistic regression, naïve bayes, random forest with ensemble classifiers using boosting technique.

An extensive review is done on the existing and proposed models for credit card fraud detection and has done a comparative study on these techniques. So Different classification models are applied to the data and the model performance is evaluated on the basis of quantitative measurements such as accuracy, precision, recall, f1 score, support, confusion matrix.

ACKNOWLEDGEMENT

Success in life is never attained single handedly. My deepest gratitude goes to my thesis supervisor, Mr. Prashant Aggarwal (Associate Professor) for their guidance, help and encouragement throughout my project work. Their enlightening ideas, comments, and suggestions have guided me a lot in completing this project successfully.

Words are not enough to express my gratitude to Dr. Arun Kumar Tripathi, Professor and Head, Department of Computer Applications, for his insightful comments and administrative help at various occasions. Fortunately, I have many understanding friends, who have helped me a lot on many critical conditions.

Finally, my sincere thanks go to my family members and all those who have directly and indirectly provided me moral support and other kind of help. Without their support, completion of this work would not have been possible in time. They keep my life filled with enjoyment and happiness.

Rahul Singh Negi (2200290140120)

Raj Srivastava (2200290140121)

TABLE OF CONTENTS

Declaration	ii
Certificate	iii
Abstract	iv
Acknowledgements	v
Table of Contents	vi
List of Figures	vii
1 Introduction	1-3
1.1 Overview	1
1.2 CCFDS	2
1.3 CCFDS using ML Algorithm	2
1.4 A research paper on CCFDS	3
2 Literature Survey	4-5
3 System Requirement and Specifications	6-7
3.1 Introduction	6
3.2 Hardware Requirement	6
3.3 Software Requirement	7
3.4 Functional Requirement	7
3.5 Non-Functional Requirement	7
3.6 Performance Requirement	7
4 System Analysis	8-10
4.1 Existing System	8-9
4.2 Proposed System	9-10
5 System Design	11-15
5.1 Project Modules	11-12
5.2 System Architecture	12
5.3 Activity Diagram	12-13
5.4 Use Case Diagram	13-14
5.5 Data Flow Diagram	14-15
6 Implementation	16
6.1 Algorithm	16
7 Testing	17-18
7.1 Unit Testing	17
7.2 Validation Testing	17-18
7.3 Functional Testing	18
7.4 Integration Testing	18
8 Performance Analysis	19-20
9 Conclusion & Future Enhancement	21

LIST OF FIGURES

Figure No.	Name of Figure	Page No.
4.1	Fraud and Non-Fraud Representation	9
4.2	Decision Tree Classifier	9
4.3	Random Forest Classifier	10
4.4	XG Boost Algorithm	10
5.1	System Architecture	12
5.2	Activity Diagram	13
5.3	Use Case Diagram	14
5.4	Data Flow Diagram	15

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Nowadays, the online transactions are growing day by day in today's world. According to a website "capitaloneshopping.com" total global credit card transactions were an estimated 678 billion in the year 2022 for an average of 1.86 billion per day. And total number of credit card holder is increased to 1.25 billion in 2023. So, this is a global market and in online transaction using credit card there some of transaction of credit card is a fraud transaction but this percentage is very less in compare to overall transaction. In financial year 2021 According to "statista.com", there were around 2021 two billion transaction transactions made via credit card across India. Fraudsters use several techniques to do fraud either they stole credit card information from credit card user or either they block the user's access to their credit card and after that use that credit card for personal gain. Sometime people report it to Bureau and sometimes they don't bother about that fraud.

The rise of digital payment methods has increased the risk of credit card fraud, making it easier for criminals to carry out their activities anonymously. Traditional rule-based systems used to detect fraud have become less effective as fraudsters have become more sophisticated in their approach. In response to this, researchers and practitioners have turned to machine learning and deep learning models as a more effective way of detecting fraudulent activities.

Credit Card Fraud Detection System is a set of methods and technique used to detect and block fraudulent purchase in on-line and from the store as well

There is dataset in our project from Kaggle to predict either transaction is fraud or it is valid transaction. This project is based on Machine Learning and trained according to the dataset, dataset is of Europe Credit Card transactions and distinguished as valid and fraud transaction on 0 and 1. This type of largely imbalance because the fraud transaction is much lower than the valid transactions which may create problem, like sometimes valid transaction is misinterpreted as fraud transactions.

1.2 CREDIT CARD FRAUD DETECTION SYSTEM

The paper discusses the problem of credit card fraud and highlights the importance of detecting fraudulent transactions promptly. The authors then present their proposed model, which involves pre-processing the transaction data and then applying various machine learning algorithms, such as logistic regression, decision trees, and random forests, to classify transactions as either fraudulent or non-fraudulent. The authors evaluate the performance of their model using a dataset of credit card transactions and compare it to other models, such as neural networks and support vector machines. The results show that the proposed model performs better than the other models in terms of accuracy, precision, and recall. The paper also discusses the limitations of the proposed model, such as the need for a large amount of data and the challenges associated with handling imbalanced datasets. The authors conclude by highlighting the potential of machine learning techniques in credit card fraud detection and the need for further research in this area.

1.3 CREDIT CARD FRAUD DETECTION USING ML ALGORITHM

The authors present their proposed model, which involves pre-processing the transaction data and then applying a CNN for feature extraction and classification. To improve the performance of the model, the authors also use feature selection techniques to identify the most relevant features for fraud detection. They evaluate the performance of their model using a dataset of credit card transactions and compare it to other models, such as logistic regression and decision trees. The results show that the proposed model performs better than the other models in terms of accuracy, precision, and recall. The authors also analyse the contribution of different features to fraud detection and discuss the limitations of the proposed model, such as the need for a large amount of data and the challenges associated with handling imbalanced datasets.

1.4 A RESEARCH PAPER ON CREDIT CARD FRAUD DETECTION

The proposed model involves pre-processing the credit card transaction data and then applying various machine learning algorithms, such as Decision Trees, Random Forest, K-Nearest Neighbour, Naive Bayes, and Artificial Neural Networks, to classify transactions as either fraudulent or non-fraudulent. The authors evaluate the performance of their model using a dataset of credit card transactions and compare it with other existing models, such as Logistic Regression, Support Vector Machine, and Gradient Boosting Machine. The results show that the proposed model outperforms the other models in terms of accuracy, precision, recall, and F1-score. The paper also discusses the challenges associated with credit card fraud detection, such as the need for real-time detection, the challenges of handling imbalanced datasets, and the importance of feature selection for improving the performance of the model.

1.5 CREDIT CARD FRAUD DETECTION PREDICTIVE MODELLING

The paper covers different machine learning techniques such as supervised, unsupervised, semi-supervised, and deep learning, and how they are applied in credit card fraud detection. The authors provide a detailed explanation of each technique, including its advantages and limitations, and also present a comparative analysis of various machine learning techniques in terms of their performance metrics. The paper also discusses the challenges associated with credit card fraud detection, such as imbalanced datasets, the need for real-time detection, and the importance of feature selection for improving the performance of the model. The authors conclude the paper by highlighting the potential of machine learning techniques in credit card fraud detection and the need for further research in this area.

1.6 A MACHINE LEARNING BASED ON CREDIT CARD FRAUD DETECTION USING THE GA ALGORITHM FOR FEATURE SELECTION

The paper covers different deep learning techniques, such as deep neural networks, convolutional neural networks, recurrent neural networks, and auto encoders, and how they are applied in credit card fraud detection. The authors provide a detailed explanation of each technique, including their advantages and limitations. The paper also presents a comprehensive analysis of different studies that have used deep learning approaches for credit card fraud detection. The authors provide a detailed summary of each study, including the dataset used, the deep learning technique applied, and the performance metrics obtained.

CHAPTER 2

LITERATURE SURVEY

2.1 Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective

Authors: Samaneh Sorournejad, Zahra Zojaji, Amir Hassan Monadjemi.

In this paper, after investigating difficulties of credit card fraud detection, we seek to review the state of the art in credit card fraud detection techniques, datasets and evaluation criteria.

Disadvantages

- Lack of standard metrics

2.2 Detection of credit card fraud: State of art

Authors: Imane Sadgali, Nawal Sael, Faouzia Benabbau

In this paper, we propose a state of the art on various techniques of credit card fraud detection. The purpose of this study is to give a review of implemented techniques for credit card fraud detection, analyses their incomes and limitless, and synthesize the finding in order to identify the techniques and methods that give the best results so far.

Disadvantages

- Lack of adaptability

2.3 Credit card fraud detection using Machine Learning Algorithm

Authors: Vaishnavi Nath Dornadulaa, Geetha S

The main aim of the paper is to design and develop a novel fraud detection method for Streaming Transaction Data, with an objective, to analyse the past transaction details of the customers and extract the behavioural patterns.

Disadvantages

- Imbalanced Data

2.4 Fraudulent Transaction Detection in Credit Card by Applying Ensemble Machine Learning techniques

Authors: Debachudamani Prusti, Santanu Kumar Rath

In this study, the application of various classification models is proposed by implementing machine learning techniques to find out the accuracy and other performance parameters to identify the fraudulent transaction.

Disadvantages

- Overlapping data.

2.5 Detection of Credit Card Fraud Transactions using Machine Learning Algorithms and Neural Networks

Authors: Deepti Dighe, Sneha Patil, Shrikant Kokate

Credit card fraud resulting from misuse of the system is defined as theft or misuse of one's credit card information which is used for personal gains without the permission of the card holder. To detect such frauds, it is important to check the usage patterns of a user over the past transactions. Comparing the usage pattern and current transaction, we can classify it as either fraud or a legitimate transaction.

Disadvantages

- Different misclassification importance

2.6 Credit card fraud detection using machine learning algorithms and cyber security

Authors: JiatongShen

As they have the same accuracy the time factor is considered to choose the best algorithm. By considering the time factor they concluded that the Ad boost algorithm works well to detect credit card fraud.

Disadvantages

- Accuracy is not getting perfectly

CHAPTER 3

SYSTEM REQUIREMENTS AND SPECIFICATIONS

3.1 SYSTEM REQUIREMENT SPECIFICATIONS

System Requirement Specification (SRS) is a fundamental document, which forms the foundation of the software development process. The System Requirements Specification (SRS) document describes all data, functional and behavioural requirements of the software under production or development. An SRS is basically an organization's understanding (in writing) of a customer or potential client's system requirements and dependencies at a particular point in time (usually) prior to any actual design or development work. It's a two- way insurance policy that assures that both the client and the organization understand the other's requirements from that perspective at a given point in time. The SRS also functions as a blueprint for completing a project with as little cost growth as possible. The SRS is often referred to as the "parent" document because all subsequent project management documents, such as design specifications, statements of work, software architecture specifications, testing and validation plans, and documentation plans, are related to it. It is important to note that an SRS contains functional and non-functional requirements only. It doesn't offer design suggestions, possible solutions to technology or business issues, or any other information other than what the development team understands the customer's system requirements.

3.2 HARDWARE SPECIFICATION

- RAM: 4GB and Higher
- Processor: Intel i3 and above
- Hard Disk: 100 GB minimum

3.3 SOFTWARE SPECIFICATION

- Operating System: Window and Linux
- Python IDE: python 2.7 and above
- Jupyter Notebook
- Programming Language: Python

3.4 FUNCTIONAL REQUIREMENTS

Functional Requirement defines a function of a software system and how the system must behave when presented with specific inputs or conditions. These may include calculations, data manipulation and processing and other specific functionality. In this system following are the functional requirements:

- Collect the Datasets
- Train the Model
- Predict the Results

3.5 NON-FUNCTIONAL REQUIREMENTS

- The system should be easy to maintain.
- The system should be compatible with different platforms.
- The system should be fast as customers always need speed.
- The system should be accessible to online users.
- The system should be easy to learn by both sophisticated and novice users.
- The system should provide easy, navigable and user-friendly interfaces.

3.6 PERFORMANCE REQUIREMENT

Performance is measured in terms of the output provided by the application. Requirement specification plays an important part in the analysis of a system. Only when the requirement specifications are properly given, it is possible to design a system, which will fit into required environment. It rests largely with the users of the existing system to give the requirement specifications because they are the people who finally use the system. This is because the requirements have to be known during the initial stages so that the system can be designed according to those requirements. It is very difficult to change the system once it has been designed and on the other hand designing a system, which does not cater to the requirements of the user, is of no use.

CHAPTER 4

SYSTEM ANALYSIS

Systems analysis is the process by which an individual studies a system such that an information system can be analysed, modelled, and a logical alternative can be chosen. Systems analysis projects are initiated for three reasons: problems, opportunities, and directives.

4.1 EXISTING SYSTEM

- Since the credit card fraud detection system is a highly researched field, there are many different algorithms and techniques for performing the credit card fraud detection system.
- One of the earliest systems is CCFD system using Markov model. Some other various existing algorithms used in the credit cards fraud detection system includes Cost sensitive decision tree (CSDT).
- Credit card fraud detection (CCFD) is also proposed by using neural networks. The existing credit card fraud detection system using neural network follows the whale swarm optimization algorithm to obtain an incentive value.
- It the uses BP network to rectify the values which are found error.

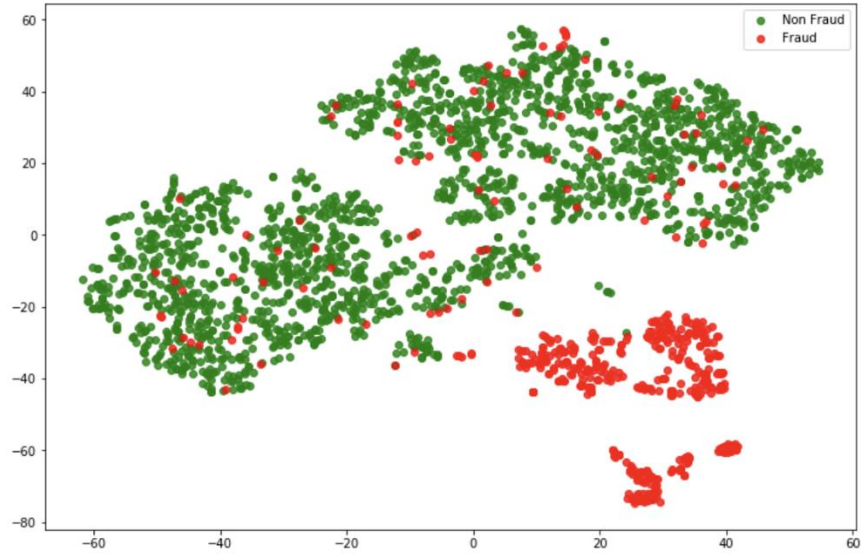


Figure 4.1: Fraud and Non-Fraud Representation

4.2 PROPOSED SYSTEM

Decision Tree:

A decision tree is a type of supervised machine learning used to categorize or make predictions based on how a previous set of questions were answered. The model is a form of supervised learning, meaning that the model is trained and tested on a set of data that contains the desired categorization.

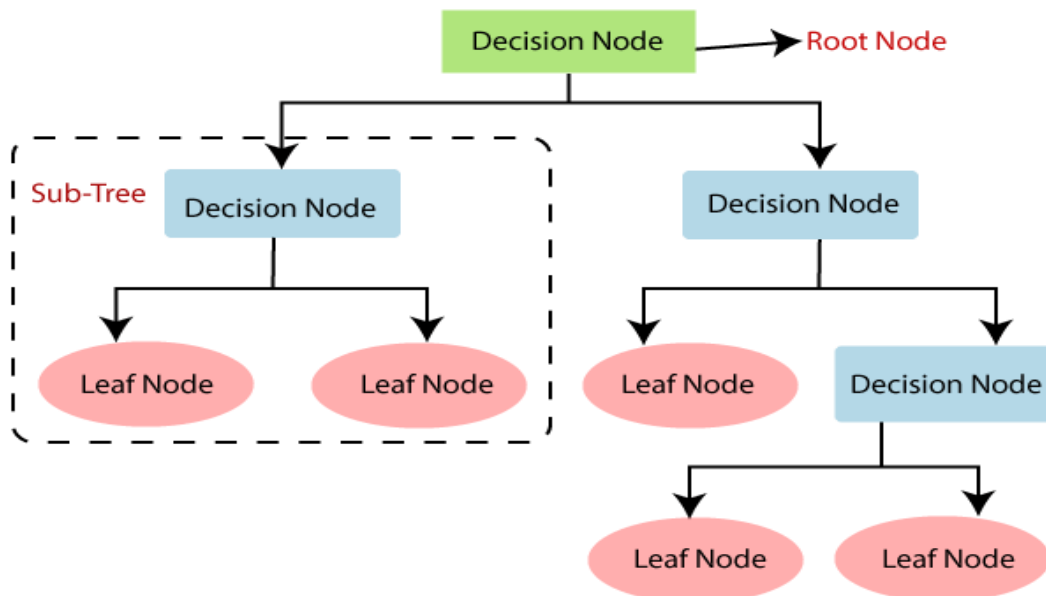


Figure 4.2: Simplified Decision Tree Classifier

Random Forest Classifier:

Features are cheekbone to jaw width, width to upper facial height ratio, perimeter to area ratio, eye size, lower face to face height ratio, face width to lower face height ratio and mean of eyebrow height. The extracted features are normalized and finally subjected to support regression.

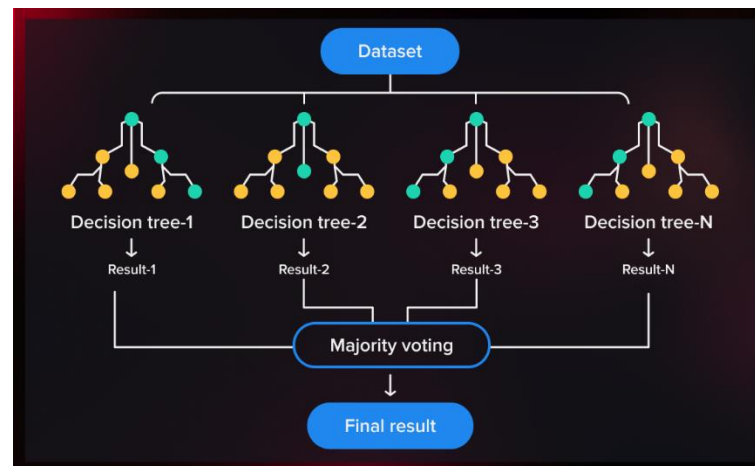


Figure 4.3: Simplified Random Forest Classifier

XG Boost Algorithm:

XG Boost stands for “Extreme Gradient Boosting” and is an implementation of Gradient Boosted decision trees.

In this algorithm, decision trees are created in sequential form. Weights play an important role in XG Boost. Weights are assigned to all the independent variables which are then fed into the decision tree which predicts results. The weight of variables predicted wrong by the tree is increased.

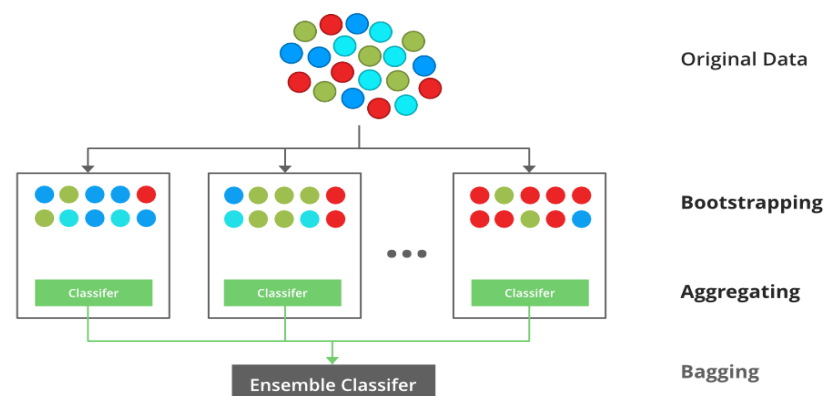


Figure 4.4: XG Boost Algorithm

CHAPTER 5

SYSTEM DESIGN

5.1 PROJECT MODULES

Module 1: Data Gathering and Data Pre-Processing

- a. A proper dataset is searched among various available ones and finalized with the dataset.
- b. The dataset must be pre-processed to train the model.
- c. In the preprocessing phase, the dataset is cleaned and any redundant values, noisy data and null values are removed.
- d. The Pre-processed data is provided as input to the module.

Module 2: Feature Engineering Module

This module extracts features from the pre-processed transaction data that can be used to predict fraud. For example, features such as the average transaction amount, the number of transactions made in a foreign country, and the number of transactions made at the same merchant in a short period of time can be extracted.

Module 3: Training the Model

- a. The Pre-processed data is split into training and testing datasets in the 80:20 ratio to avoid the problems of over-fitting and under-fitting.
- b. A model is trained using the training dataset with the following algorithms SVM, Random Forest Classifier and Decision Tree.
- c. The trained models are trained with the testing data and results are visualized using bar graphs, scatter plots.
- d. The accuracy rates of each algorithm are calculated using different params like F1 score, Precision, Recall. The results are then displayed using various data visualization tools for analysis purpose.

Module 4: Model Evaluation Module

The accuracy rates of each algorithm are calculated using different params like F1 score, Precision, Recall. The results are then displayed using various data visualization tools for analysis purpose.

5.2 SYSTEM ARCHITECTURE

Our Project main purpose is to making Credit Card Fraud Detection awaring to people from credit card online frauds. the main point of credit card fraud detection system is necessary to safe our transactions & security. With this system, fraudsters don't have the chance to make multiple transactions on a stolen or counterfeit card before the cardholder is aware of the fraudulent activity. This model is then used to identify whether a new transaction is fraudulent or not. Our aim here is to detect 100% of the fraudulent transactions while minimizing the incorrect fraud classifications.

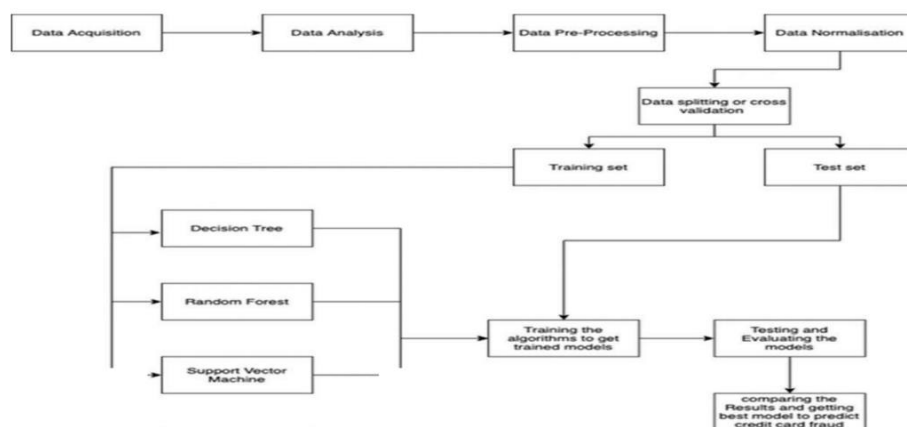


Figure 5.1: System Architecture

5.3 ACTIVITY DIAGRAM

Activity diagram is an important diagram in UML to describe the dynamic aspects of the system. Activity diagram is basically a flowchart to represent the flow from one activity to another activity. The activity can be described as an operation of the system. The control flow is drawn from one operation to another. This flow can be sequential, branched, or concurrent. Activity diagrams deal with all type of flow control by using different elements such as fork, join, etc. The basic purposes of activity diagram are it captures the dynamic behaviour of the system. Activity diagram is used to show message flow from one activity to another Activity is a particular operation of the system. Activity diagrams are not only used for visualizing the dynamic nature of a system, but they are also used to construct the executable

system by using forward and reverse engineering techniques. The only missing thing in the activity diagram is the message part.

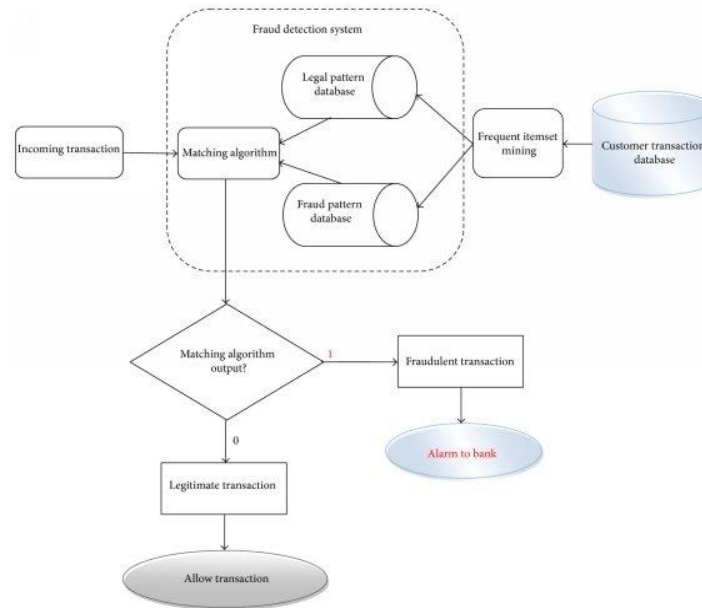


Figure 5.2: Activity Diagram

5.4 USE CASE DIAGRAM

In UML, use-case diagrams model the behaviour of a system and help to capture the requirements of the system. Use-case diagrams describe the high-level functions and scope of a system. These diagrams also identify the interactions between the system and its actors. The use cases and actors in use-case diagrams describe what the system does and how the actors use it, but not how the system operates internally. Use-case diagrams illustrate and define the context and requirements of either an entire system or the important parts of the system. You can model a complex system with a single use-case diagram, or create many use-case diagrams to model the components of the system. You would typically develop use-case diagrams in the early phases of a project and refer to them throughout the development process.

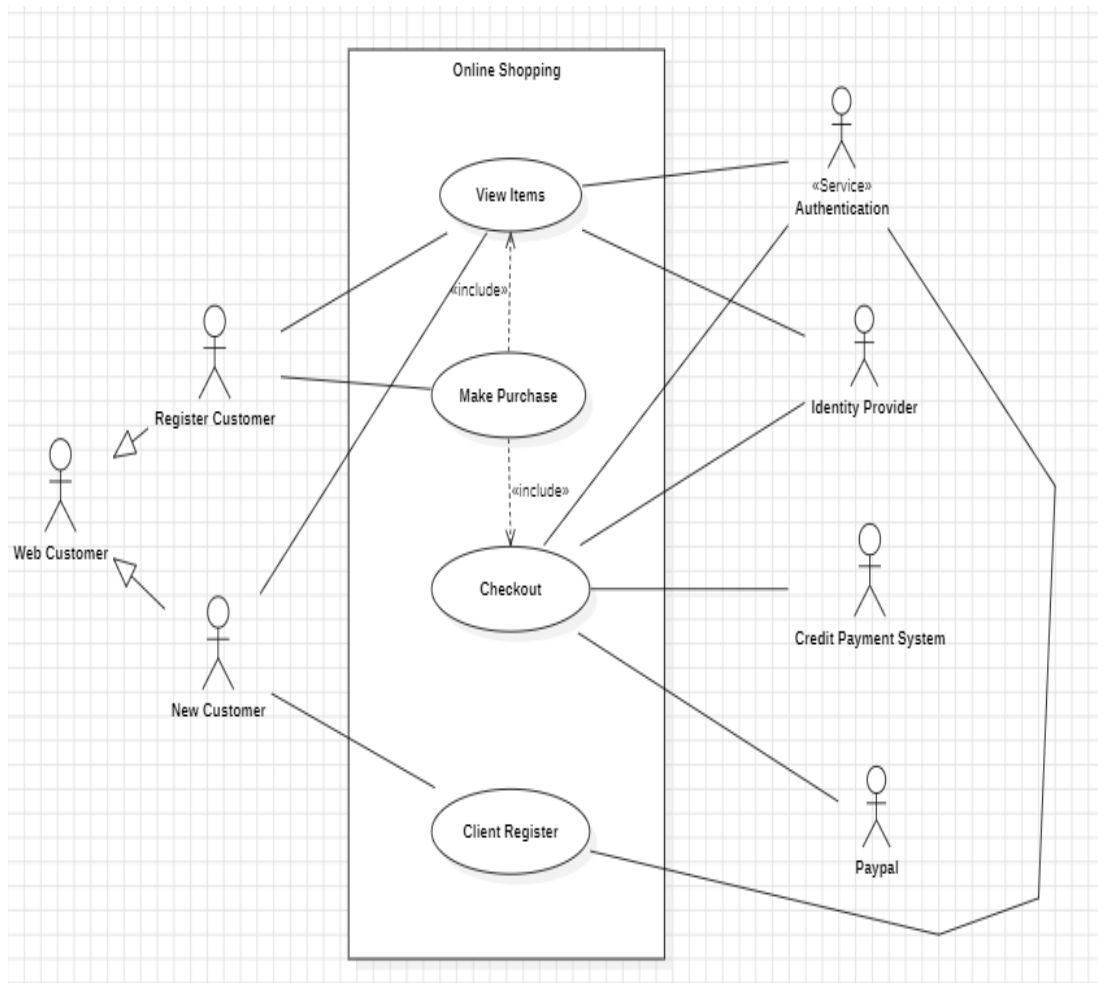


Figure 5.3: Use Case Diagram

5.5 DATA FLOW DIAGRAM

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It can be manual, automated, or a combination of both. It shows how data enters and leaves the system, what changes the information, and where data is stored. The objective of a DFD is to show the scope and boundaries of a system as a whole. It may be used as a communication tool between a system analyst and any person who plays a part in the order that acts as a starting point for redesigning a system. The DFD is also called as a data flow graph or bubble chart.

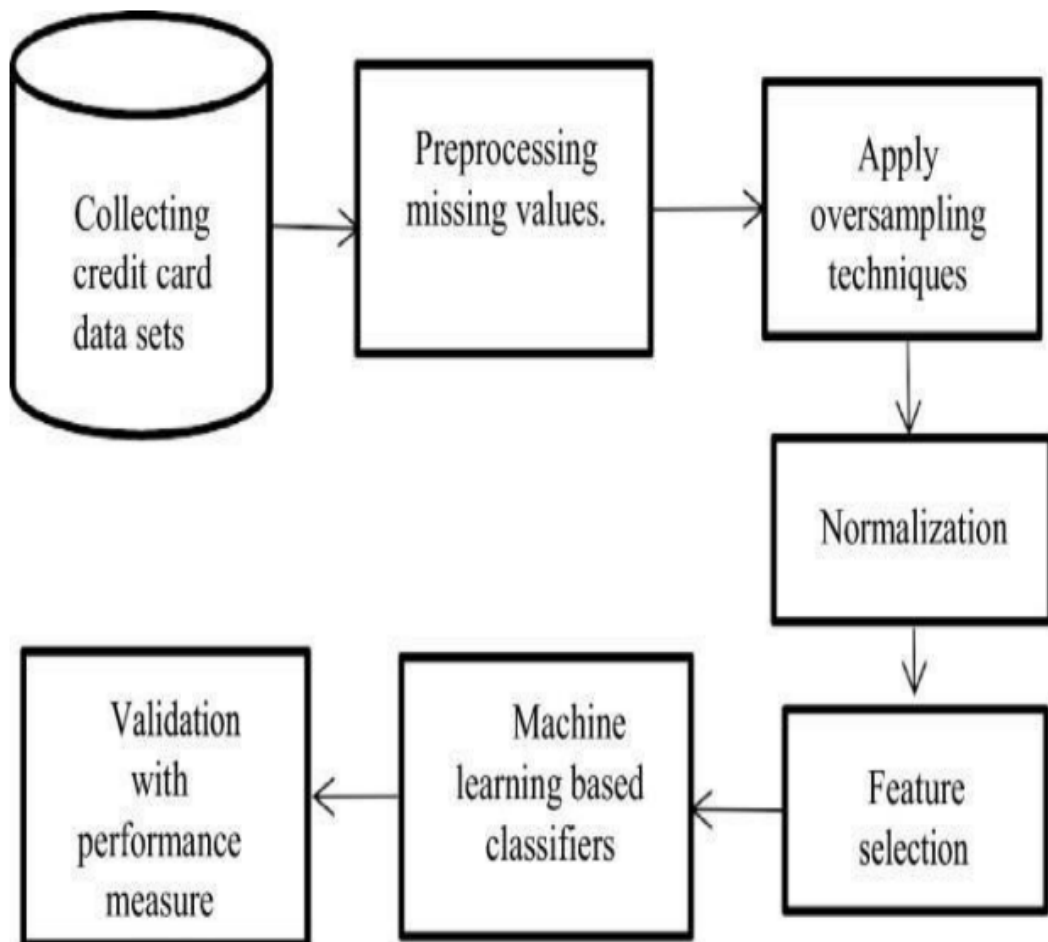


Figure 5.4: Flow Diagram

CHAPTER 6

IMPLEMENTATION

6.1 ALGORITHM

Step 1: Import dataset

Step 2: Convert the data into data frames format

Step3: Do random oversampling using ROSE package

Step4: Decide the amount of data for training data and testing data

Step5: Give 80% data for training and remaining data for testing.

Step6: Assign train dataset to the models

Step7: Choose the algorithm among 3 different algorithms and create the model

Step8: Make predictions for test dataset for each algorithm

Step9: Calculate accuracy for each algorithm

Step10: Apply confusion matrix for each variable Step11: Compare the algorithms for all the variables and find out the best algorithm

CHAPTER 7

TESTING

Testing is a process of executing a program with intent of finding an error. Testing presents an interesting anomaly for the software engineering. The goal of the software testing is to convince system developer and customers that the software is good enough for operational use. Testing is a process intended to build confidence in the software. Testing is a set of activities that can be planned in advance and conducted systematically. Software testing is often referred to as verification & validation.

7.1 UNIT TESTING

In this testing we test each module individually and integrate with the overall system. Unit testing focuses verification efforts on the smallest unit of software design in the module. This is also known as module testing. The module of the system is tested separately. This testing is carried out during programming stage itself. In this testing step each module is found to working satisfactorily as regard to the expected output from the module. There are some validation checks for fields also. It is very easy to find error debut in the system.

7.2 VALIDATION TESTING

At the culmination of the black box testing, software is completely assembled as a package, interfacing errors have been uncovered and corrected and a final series of software tests. Asking the user about the format required by system tests the output displayed or generated by the system under consideration. Here the output format is

considered the of screen display. The output format on the screen is found to be correct as the format was designed in the system phase according to the user need. For the hard copy also, the output comes out as specified by the user. Hence the output testing does not result in any correction in the system.

7.3 FUNCTIONAL TESTING

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals. Functional testing is centred on the following items: Valid Input: identified classes of valid input must be accepted. Invalid Input: identified classes of invalid input must be rejected. Functions: identified functions must be exercised. Output: identified classes of application outputs must be exercised. Systems/Procedures: interfacing systems or procedures must be invoked. Organization and preparation of functional tests is focused on requirements, key functions, or special test cases Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

7.4 INTEGRATION TESTING

Data can be lost across an interface; one module can have an adverse effort on the other sub functions when combined may not produces the desired major functions. Integrated testing is the systematic testing for constructing the uncover errors within the interface. The testing was done with sample data. The Developed system has run successfully for this sample data. The need for integrated test is to find the overall system performance.

7.5 USER ACCEPTANCE TESTING

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements. Some of my friends were who tested this module suggested that this was really a user-friendly application and giving good processing speed.

CHAPTER 8

PERFORMANCE ANALYSIS

8.1 PERFORMANCE METRICS

The basic performance measures derived from the confusion matrix. The confusion matrix is a 2 by 2 matrix table contains four outcomes produced by the binary classifier. Various measures such as sensitivity, specificity, accuracy and error rate are derived from the confusion matrix.

ACCURACY

Accuracy is calculated as the total number of two correct predictions(A+B) divided by the total number of the dataset(C+D). It is calculated as (1-error rate).
$$\text{Accuracy} = \frac{A+B}{C+D}$$
Whereas,

A=True Positive B=True Negative

C=Positive D=Negative

ERROR RATE

Error rate is calculated as the total number of two incorrect predictions(F+E) divided by the total number of the dataset(C+D).

$$\text{Error rate} = \frac{F+E}{C+D}$$
Whereas,

E=False Positive F=False Negative

C=Positive D=Negative

SENSITIVITY

Sensitivity is calculated as the number of correct positive predictions(A) divided by the total number of positives(C).

$$\text{Sensitivity} = A/C$$

SPECIFICITY

Specificity is calculated as the number of correct negative predictions(B) divided by the total number of negatives(D).

$$\text{Specificity} = B/D.$$

CHAPTER 9

CONCLUSION & FUTURE ENHANCEMENT

CONCLUSION

Nowadays, in the global computing environment, online payments are important, because online payments use only the credential information from the credit card to full fill an application and then deduct money. Due to this reason, it is important to find the best solution to detect the maximum number of frauds in online systems. Accuracy, Error-rate, Sensitivity and Specificity are used to report the performance of the system to detect the fraud in the credit card. In this paper, three machine learning algorithms are developed to detect the fraud in credit card system. To evaluate the algorithms, 80% of the dataset is used for training and 20% is used for testing and validation. Accuracy, error rate, sensitivity and specificity are used to evaluate for different variables for three algorithms. The accuracy result is shown for SVM; Decision tree and random forest classifier are 99.94, 99.92, and 99.95 respectively. The comparative results show that the Random Forest performs better than the SVM and decision tree techniques.

FUTURE ENHANCEMENT

Detection, we did end up creating a system that can, with enough time and data, get very close to that goal. As with any such project, there is some room for improvement here. The very nature of this project allows for multiple algorithms to be integrated together as modules and their results can be combined to increase the accuracy of the final result. This model can further be improved with the addition of more algorithms into it.