

Detection of Fraudulent Credit Card Transactions using Classification Algorithms

¹Suchitra Vishnu Naik, ²Prof. Saravanan C

¹Student, Department of MCA, RV College of Engineering®, Bengaluru, India

²Assistant Professor, Department of MCA, RV College of Engineering®, Bengaluru, India

Abstract

Credit cards are widely used in our daily life due to development of mobile applications. In this present technology payment methods are mainly concentrated on online payments by the huge development in the internet services globally. Almost every company and industries have changed their traditional system into online services to provide e-commerce system. Hence this system leads towards less time and more profitability, it is also having major short comings. One of the crucial challenges in

making this online payment is credit card fraud. This online payment through credit card will lead to carry an anonymous fraudulent transaction by fraudsters. To overcome this problem, credit card fraud detection using classification algorithms is proposed with Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbor (K-NN) and Naive Bayes (NB) algorithms. The results compared in pie graph.

Keywords: Credit card, Random Forest, K-Nearest Neighbor, Support Vector Machine, Naive Bayes.

I. INTRODUCTION

Credit Card is a card given to clients to arrange an installment policy through the card. These cards are used by the card owners to purchase merchandise or ventures. Online shopping is having huge extension in the business process and in all kind of buying's and purchasing [1]. So, the number of credit card exchanges having significant ascent in fake exercise.

Almost every companies are switched the business from traditional transaction system into online services to make the access easier to the customers. This system is having more gain fullness, yet it is having some weakness. Subsequently, a misrepresentation recognition framework

including different discovery procedures is a lot of basic for

the financial establishments to continue the altruism from the clients [2].

II. LITERATURE SURVEY

There are some applications which is already existed to check the fraud in credit cards. Some of the existing applications are:

[1] This paper explains about proposed prescient classification model by mixing the other models. The gathering of AI calculations helps to enhance the exhibitions notably. The outcome has examined and

seen that the precision estimation of the proposed model is significantly high when contrasted with singular classification models [1].

[2] This paper explains about the favorable circumstances, inconveniences of the machine learning calculations have been talked about alongside examination of various calculations (at every possible opportunity) as far as execution, learning rate and so on [2].

[3] This paper explained about utilized Irregular Timberland Calculation and sensory systems for relapse of dataset. To begin with, they have gathered the Mastercard dataset and investigated. In this examination the precision of Mastercard misrepresentation exchanges can be acquired which will be at last spoken to as graphical portrayal [3].

[4] This paper explained about the case of clustering assists with improving the prescient presentation of Visa extortion. By designing helpful and graphic highlights at the record level, the theory will have the option to isolate important groups that will improve forecast capacities [4].

[5] This paper explains about utilizing facts mining alongside sensory system, the accomplishment pace of the framework supplements numerous bunches and subsequently will comprehend the motivation behind supporting the traders [5].

[6] This paper explains about a SIP-based enemy of extortion system that depends on client profiling. This system incorporates a Bayesian Belief Network model that is prepared from breaking down legitimate CDR information to assemble a contingent likelihood table [6].

[7] This paper clarifies about the utilization of earlier likelihood got from preparing set yielded a superior arrangement execution than uniform likelihood. It shows that the decent variety of earlier likelihood esteems that each class holds is very significant for execution of the classifier [7].

[8] This paper clarifies about test time of PHNB is fundamentally diminished on high dimensional datasets, in the meantime the precision of which is like HNB, considerably higher on some specific datasets [8].

[9] This paper clarifies about a first consequences of a correlation among SVM, IVM and RVM for a classification of hyperspectral HyMap information. We purposefully utilized a little preparing informational collection and countless classes [9].

III. PURPOSE

Credit cards are widely used in our daily life due to development of mobile applications. Online payment method need not requires a physical card to complete the transaction. By applying classification algorithms, the models help to identify number of fraudulent transactions, Valid transactions, Ratio of fraudulent transactions, Precision score, Recall score and Accuracy score.

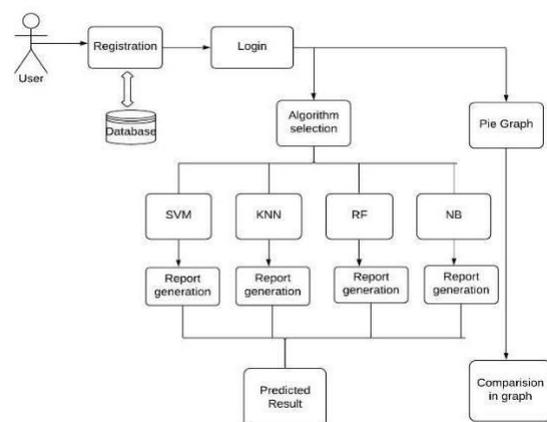


Figure 1- Block diagram

Figure-1 explains about the block diagram of the Credit Card Fraud Detection (CCFD) system using classification algorithm. First user needs to register to the system with details like username, password, email and phone no. The user details will get stored into the database. After registration, user can login to the system with registered user details. After that user gets two options such as algorithm selection and Pie graph Representation.

IV. PROPOSED METHODOLOGY

Proposed system is implemented using K-NN, RF, SVM, NB classifier for classification of dataset. Existing dataset is referred from the internet. After collecting the dataset, divided the dataset as Prepared and Testing set for training purpose. In partitioning, the classification algorithms like K-NN, RF, SVM, and NB classifier are applied, and these calculations provides best precision about the fraud transactions and analyzes every calculation and used to distinguish the proficient calculation. In this analysis the accuracy represented in the form of graphical representation to show the comparison of each algorithm.

V. IMPLEMENTATION

The framework is created utilizing python Tkinter to give GUI of the implemented project. SQLyog is the database used to store the user details. The dataset is trained with classification algorithms and result gets predicted to show the number of fraudulent transactions and valid transactions.

Implemented Result

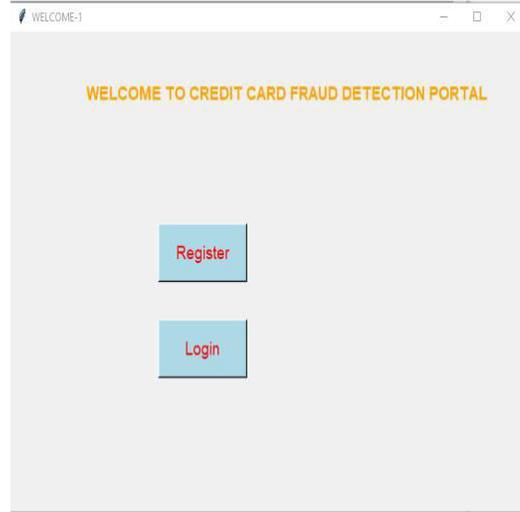


Fig 2- Credit card fraud detection portal

Figure-2 shows the home page of CCFD system, which gets opened after the running of the program. This page contains two buttons such as Register and Login. Register button is used to register the new users with their details and Login button is used to allow the authenticated user to access the portal.

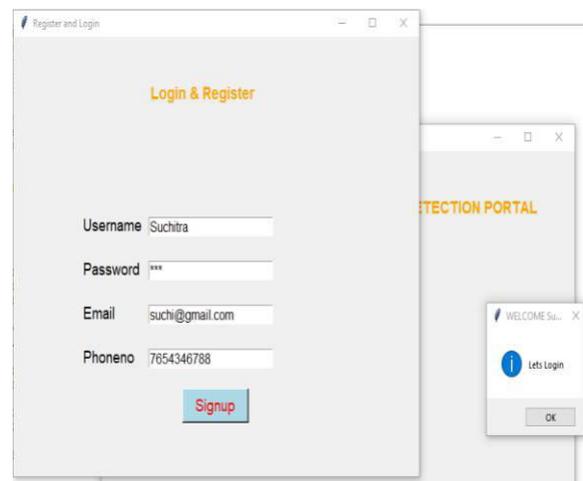


Figure 3- Registering with valid user details

Figure-3 shows, entering the user details for registration. For Registration process user should enter valid Username, Password, Email and Phone number. The entered valid details will get stored into the database.

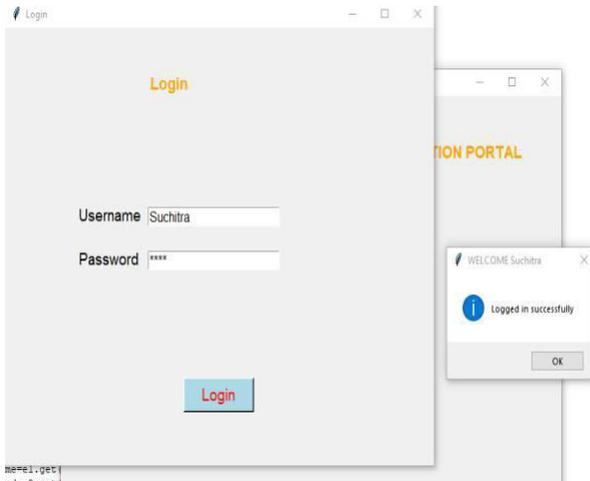


Figure 4- Logging in with authenticated user details

Figure 4 shows the login page, which allows registered user to access the CCFD system with authenticated details. User who is trying to access the system should enter authenticated username and password. This page will not allow any unauthenticated user to access the system.

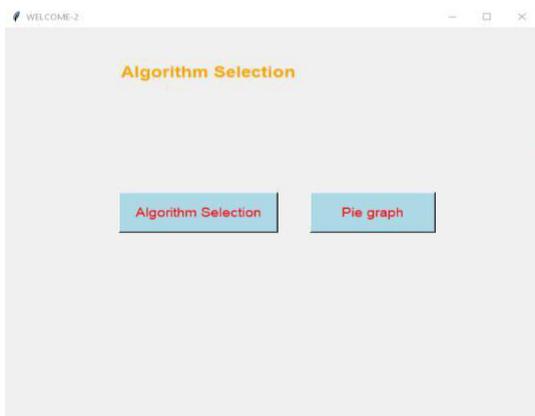


Figure 5- Selecting algorithms or pie chart

Figure 5 shows the credit card fraud detection system which consists two buttons such as Algorithm Selection and Pie graph. The authenticated user should select algorithm selection button to select the algorithm among four different algorithms

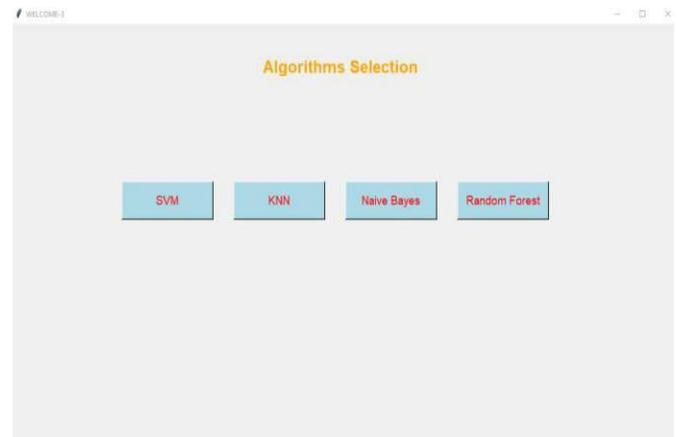


Figure 6- Algorithm selection

Figure 6 is an algorithm selection page which is having four buttons such as SVM, KNN, Naïve Bayes and Random Forest. The four buttons is used to train the dataset with four different algorithm to predict the result.

```

===== RESTART: D:\Credit Card Fraud Detection\code\credit code.py =====
##-----SVM ALGORITHM-----##

The number of Fraudulent transactions(Class 1) are: 492

The number of Valid transactions(Class 0) are: 284315

The ratio of Fraudulent transactions is: 0.001727485630620034

Precision Score: 1.0

Recall Score: 1.0

Accuracy Score: 1.0
    
```

Figure 7- Result of SVM algorithm

Figure 7 shows the result of CCFD system with SVM algorithm. The algorithm shows the no. of valid transactions, no. of frauded transactions, ratio of frauded transactions, Precision score, Recall score and Accuracy score.

transactions, num of frauded transactions, ratio of frauded transactions, Precision score, Recall score and Accuracy score.

```
##-----KNN ALGORITHM-----##
The number of Fraudulent cases is: 492
The number of valid transactions is: 284315
The ratio of fraudulent transactions is: 0.001727485630620034
Precision Score: 0.8888888888888888
Recall Score: 0.05925925925925926
Accuracy Score: 0.9982022976882672
```

```
##-----RANDOM FOREST ALGORITHM-----##
The number of Fraudulent transactions is: 492
The number of Valid transactions is: 284315
The ratio of fraudulent transactions is: 0.001727485630620034
Precision Score: 0.9381443298969072
Recall Score: 0.6893939393939394
Accuracy Score: 0.9993399061824106
```

Figure 8 – Result of KNN algorithm

Figure 9- Result of Random Forest algorithm

Figure 8 shows the result of CCFD system with K-NN algorithm. The algorithm shows the num of valid transactions, num of frauded transactions, ratio of frauded transactions, Precision score, Recall score and Accuracy score

Figure 9 shows the result of CCFD system with RF algorithm. The algorithm shows the num of valid exchanges, num of frauded exchanges, ratio of fraudulent transactions, Precision score, Recall score and Accuracy score.

```
===== RESTART: D:\Credit Card Fraud Detection\code\ccredit code.py =====
##-----NAIVE BAYES ALGORITHM-----##
The number of Fraudulent transactions(Class 1) are: 492
The number of Valid transactions(Class 0) are: 284315
The ratio of fraudulent transactions is: 0.001727485630620034
Precision Score: 1.0
Recall Score: 1.0
Accuracy Score: 1.0
```

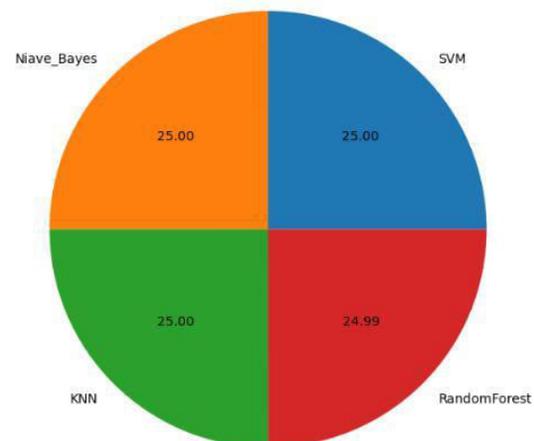


Figure 8- Result of Naïve Bayes Algorithm

Figure 10- Comparison in pie graph

Figure 8 shows the result of CCFD system with NB algorithm. The algorithm shows the num of valid

The Figure 10 shows the comparison of four calculations such as SVM, K-NN, NB and RF algorithm's result in a pie graph.

VI. CONCLUSION

Effective CCFD framework is a most extreme prerequisite for any card giving bank. This has given a considerable amount of enthusiasm from the examination network and a few strategies proposed to encounter the fraud. Credit The primary objective of this undertaking is to look at certain ML calculations for identification of fraudulent exchanges. t card frauds speak to an intense business issue.

VII. REFERENCE

- [1] Debachudamani Prusti and Santanu Kumar Rath "Fraudulent Transaction Detection in Credit Card by Applying Ensemble Machine Learning techniques", on tenth ICCCNT 2019 July 6-8, 2019, IIT - Kanpur
- [2] Susmita Ray "A Quick Review of Machine Learning Algorithms", on International Conf on Machine learning, Cloud, Big data and Parallel computing (Com-IT-Con), India, fourteenth - sixteenth Feb 2019
- [3] M. Suresh Kumar, V. Soundarya and at all "Credit card fraud detection using random forest algorithm", on third International Conf on computing and Communication Technologies ICCCT 2019
- [4] Navin Kasa, Andrew Dahbura and at all "Improving credit card fraud detection by Profiling and accounts", on eighteenth international symposium INFOTEH-JAHORINA, 20-22 March 2019 clustering
- [5] Mrs.Vimala Devi. J and Dr. Kavitha, K.S "Fraud detection in credit card transactions by using classification algorithms", on second International conf on Info technology on 2017
- [6] Aman Srivastava Mugdha Yadav and at all "Credit card fraud detection at merchant side using neural networks", on international conf on computing for sustainable global development on 2016
- [7] K. G. Co and Y. Gmbh, "global online payment methods: full year 2016," Tech. Rep., 3 2016
- [8] S. Benson Edwin Raj and A. Annie Portia "Analysis on Credit card fraud detection methods", on international conf on computer, communication and Electrical technology – ICCCET 2011, eighteenth and nineteenth March 2011
- [9] Gupta, Shalini, and R. Johari. "A new framework for credit card transactions involving mutual authentication between card holder and merchant" on International conf on Communication systems and network technologies IEEE, 2011
- [10] Seyedhossein, Leila, and M. R. Hashemi. "Mining Information from credit card time series for timelier fraud detection", International symposium on telecommunications IEEE, 2011