



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 5, May 2022

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.118

9940 572 462

6381 907 438

ijirset@gmail.com

www.ijirset.com

Credit Card Fraud Prevention & Detection using Machine Learning

Mrs.V.C.Sanap¹, Sangita Hazra², Arya Deopurkar, Ashwini Bhadane, Roshan Bacchav

Lecturer, Department of Computer Engineering, AISSMS Polytechnic, Pune, India¹

Students, Department of Computer Engineering, AISSMS Polytechnic, Pune, India²

ABSTRACT: In today's world of e-commerce where lots of offers are available, the most drawbacks for online business is to deal with credit card fraud, and it's a drain on each and every merchant's revenue to prevent credit card fraud. "Credit Card fraud detection is essentially the process of identifying purchase attempts that are fraudulent & rejecting them instead of processing the order." On daily basis, the financial transactions are made on huge amount in global market and hence detecting credit card fraud activity is challenging task. Variety of techniques as well as various tools is available for detecting frauds with most of the merchants. Card payments are very easy to use because we only need to transmit little information to bank in order to identify our account & authorize the transaction. Machine Learning plays an important role for detecting frauds in any transactions. In order to predict these transactions the banks use various machine learning methods. In this paper we have used some algorithms like SVM, Naive Bayes & Decision Tree for credit card fraud detection.

KEYWORDS: e-commerce, online business, Fraud Detection, SVM, Decision Tree, Naive Bayes, Machine Learning.

I. INTRODUCTION

Credit card fraud scrub as much as 5% of the world's GDP (Gross Domestic Product.) per annum. Combating fraud detection using AI is to detect the suspicious activities. Combating money fraud generally requires most entities that complete financial/money transactions to keep thorough records of their clients' accounts and activities. If they come across any information that appears to be suspicious, they are required to report it to the government for further investigation. In this Transaction records is check to detect money laundering activity if the suspicious data is detected. Here we have a tendency to use Machine Learning Algorithm to detect the suspicious activities and solve it by training the data of that activity. We are going to use supervised and unsupervised algorithm techniques.

II. RELATED WORK

In this project we have implemented to detect fraud using machine learning algorithms like Decision Tree, Support Vector Machine and Naive Bayes. In today's world credit card fraud cases are increasing day by day, so it is very important to understanding the technology behind frauds. Like hacker or unauthorized person. So solution for this happening crime we developed credit card fraud detection system. In this system we implement three machine learning algorithms are as follows:

1. Decision Tree:

In a decision tree is a predictive model for classification and regression problems that map the inputs to the possible classes. This supervised technique has a tree-like structure that contains root nodes, other nodes that split the data based on the features, and leaves. At each node, the classes in the data are separated based on some conditions on the features. The splitting process achieves the fullest purity. This technique is widely used for credit card fraud detections.

2. Support Vector Machine:

In a SVM is another supervised method that is applicable for classification and regression problems. This technique can handle high-dimensional data by transforming a non-linear input into a linear task. SVM has been applied to

detect fraud in banking industries.SVM creates the decision boundary to segregate the classes.

3. Naive Bayes:

Naïve Bayes algorithm is reached from Bayes theorem. This algorithm is very easy to learn and useful for large dataset like credit card dataset. in our project we use this algorithm to train dataset.

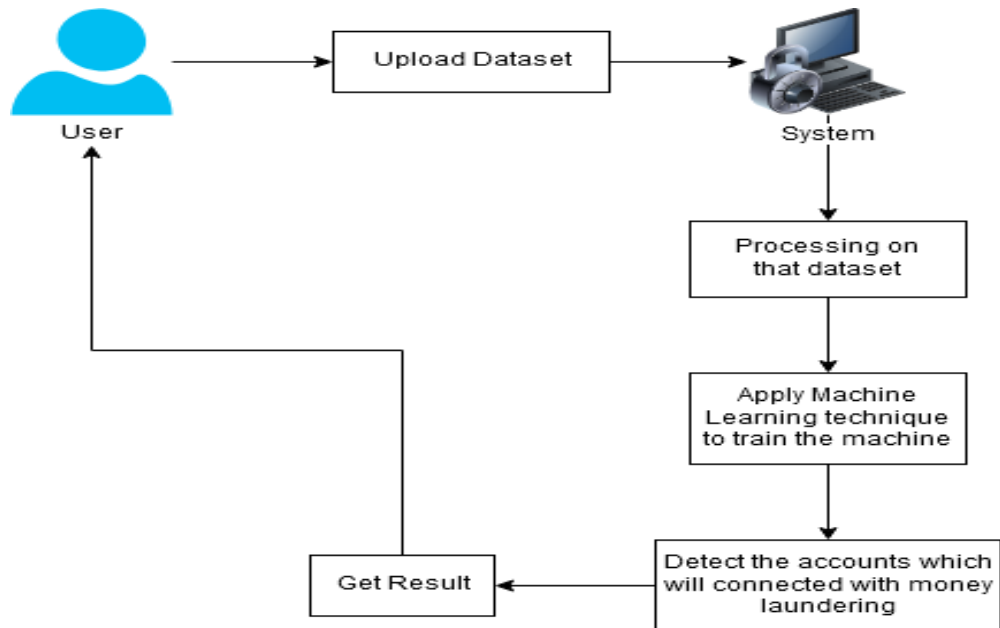


Fig.-System Architecture

III. METHODOLOGY

For Credit Card fraud detection, machine learning is very important as it plays vital role. In our project we have used various packages like Numpy that is numeric python, tkinter that provides a fast and easy way to create GUI applications, PIL that is image processing, cv2 that is used for all sorts of image and video analysis, like facial recognition and detection, sqlite3 that integrates the SQLite database with Python. We have used anaconda navigator because it has different types of IDE's, among all the IDE'S we chose "Spyder" IDE. Firstly the Login, Register & Exit button are used in the interface. We need to register first if we are new to the system else we can simply login or exit. We have created database to store credit card information, merchant information, and registration data & face data. After we login we have 3 options Card master, merchant master and face capture .In card master and merchant master we can add, edit, save ,delete and set the status as active or deactivate.Next in Face capture we can create and train face data, also user authentication is available. If authentication is successful we have to enter our email address and OTP is generated afterentering the OTP transaction page is opened where we have to purchase something and if the amount exceeds a certain limit it displays “AS FRAUD ENTRY”.

IV. EXPERIMENTAL RESULTS

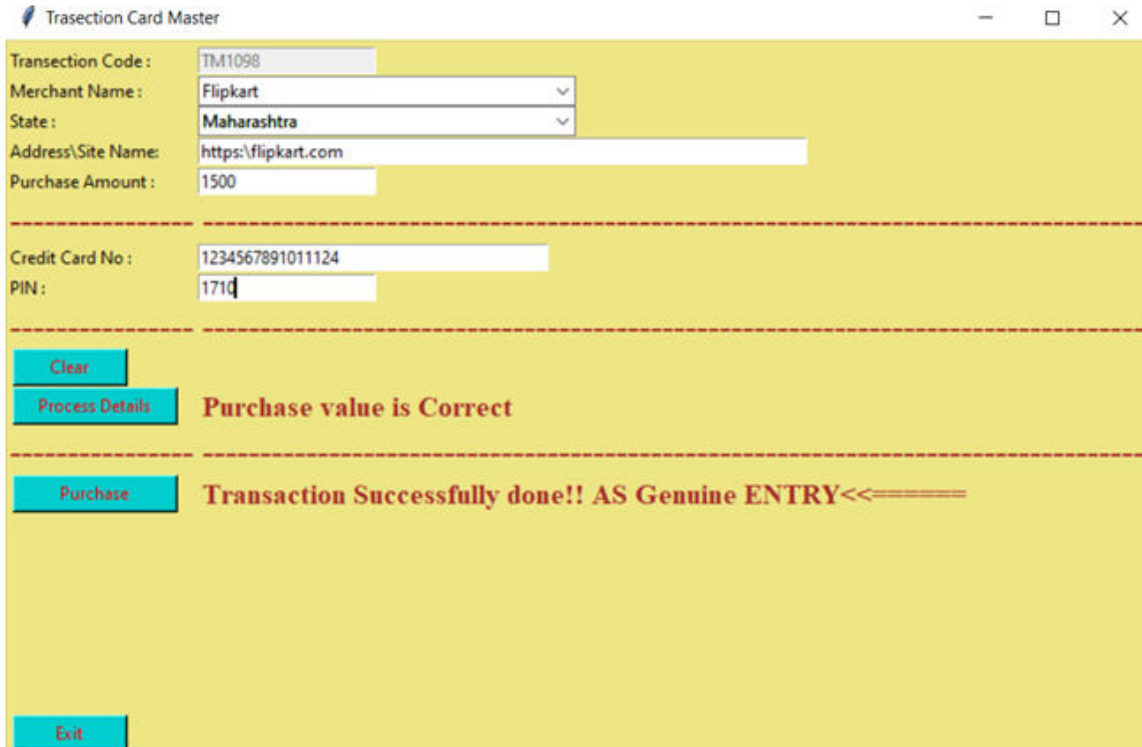
CREDIT CARD FRAUD DETECTION



Fig.- Login Registration Page.



Fig.- Credit & Merchant Master, Face Capture.



The screenshot shows a window titled "Trasection Card Master" with a yellow background. It contains several input fields and buttons. The fields are: Transaction Code (TM1098), Merchant Name (Flipkart), State (Maharashtra), Address\Site Name (https://flipkart.com), Purchase Amount (1500), Credit Card No (1234567891011124), and PIN (1710). There are four buttons: "Clear", "Process Details", "Purchase", and "Exit". The "Process Details" button is highlighted in red, and the text "Purchase value is Correct" is displayed in red. Below it, the "Purchase" button is also highlighted in red, and the text "Transaction Successfully done!! AS Genuine ENTRY<<=====" is displayed in red.

Fig.- Transaction page if genuine Entry is detected.



The screenshot shows a window titled "Trasection Card Master" with a yellow background. It contains several input fields and buttons. The fields are: Transaction Code (TM1098), Merchant Name (Flipkart), State (Maharashtra), Address\Site Name (https://flipkart.com), Purchase Amount (15000), Credit Card No (1234567891011124), and PIN (1710). There are four buttons: "Clear", "Process Details", "Purchase", and "Exit". The "Process Details" button is highlighted in red, and the text "Purchase value is Correct" is displayed in red. Below it, the "Purchase" button is also highlighted in red, and the text "Transaction Failed!! AS FRAUD ENTRY<<=====" is displayed in red.

Fig.- Transaction page if Fraud Entry is detected.



V. CONCLUSION

Credit Card frauds happens when the customer make payment or to other account which is hacked by unauthorized person. The account owner does not give permission to payment or transaction it is done by third party. Therefore we make credit card fraud detection system to detect frauds. We also used some machine learning algorithms like Support Vector machine, Decision Tree and Navies Bayes.

REFERENCES

- [1] "Fatf-gafi.org - Financial Action Task Force (FATF)", Fatf-gafi.org,2016. [Online]. Available: <http://www.Fatf-gafi.org>. [Accessed: 22-Dec- 2015].
- [2] Neo4j Graph info, 'Neo4j, the World's Leading Graph Database', 2014. [Online]. Available:<http://neo4j.com/>. [Accessed: 22- Dec- 2015].
- [3] A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten. Improving credit card fraud detection with calibratedprobabilities. In SDM, 2014.
- [4] A. Shen, R. Tong, Y. Deng, "Application of classification models on credit card fraud detection", Service Systemsand Service Management 2007 International Conference, pp. 1-4, 2007.
- [5] A. C. Bahnsen, A. Stojanovic, D. Aouada, B. Ottersten, "Cost sensitive credit card fraud detection using Bayes minimum risk", Machine Learning and Applications (ICMLA). 2013 12th International Conference, vol. 1, pp. 333-338, 2013
- [6] G. Singh, R. Gupta, A. Rastogi, M. D. S. Chandel, A. Riyaz, "A Machine Learning Approach for Detection of Fraud based on SVM", International Journal of Scientific Engineering and Technology, vol. 1, no. 3, pp. 194-198, 2012, ISSN ISSN: 2277-1581
- [7] K. Chaudhary, B. Mallick, "Credit Card Fraud: The study of its impact and detection techniques", International Journal of Computer Science and Network (IJCSN), vol. 1, no. 4, pp. 31-35, 2012, ISSN ISSN: 2277-5420
- [8] M. J. Islam, Q. M. J. Wu, M. Ahmadi, M. A. SidAhmed, "Investigating the Performance of Naive-Bayes Classifiers and KNearestNeighbor Classifiers", IEEE International Conference on Convergence Information Technology, pp. 1541-1546, 2007.
- [9] S. Patil, H. Somavanshi, J. Gaikwad, A. Deshmane, R. Badgujar, "Credit Card Fraud Detection Using Decision Tree Induction Algorithm", International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 4, no. 4, pp. 92-95, 2015, ISSN ISSN: 2320-088X.



INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 **9940 572 462**  **6381 907 438**  **ijirset@gmail.com**



www.ijirset.com

Scan to save the contact details