Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

Online Transaction Fraud Detection using Backlogging on E-Commerce Website

Swapnil Malatesh Dharnappa Goudar
Computer Science Engineering
MIT ADT University
Pune

Gyanangshu Misra
Computer Science Engineering
MIT ADT University
Pune

***Abstract*— Credit card fraud is one of the most committed crimes in today's digital era. To stop this crime from getting out of hand some sets of rules have been established to stop money from being obtained through illegal means. Now mostly, credit cards fraud happens when the fraudster has obtained the credit card information through some illegal means and then further uses it to carry out his/her nefarious goals. To detect this sort of credit card frauds researchers have used the machine learning algorithms. But the level of accuracy in these cases still has some loopholes which has yet to be mended. So, even with this advancement, fraud detection is still in a very nascent stage and more techniques with 100% efficiency still need to be developed to totally minimize the risk of credit card fraud.**

Now, the banks giving credit cards has established a fraud detection system (FDS) in which the system receives the details of the card and the transaction value which upon verification shows whether the transaction is genuine or not. If any sort of surprising pattern is detected by the FDS then it asks for a re- verification. The algorithm used in the system then analyses all previous information of that card holder and recognizes any unusual pattern in the payment procedure. It gives the user three attempts to give the correct details, failing of which the system then blocks the card and inhibits the user from completing the transaction.

***Keywords*— Credit card fraud detection, Credit Card, Machine Learning, E-commerce, Python**

I. INTRODUCTION

Now, as with each passing year more and more countries are going cashless and the dependency on online payment methods are increasing, many complicated investigation systems are being developed and used so as to identify obscure patterns and the relationships among large informational indexes which were earlier impossible to detect. This comes under a new term called Information Mining. The tools which are used in information mining are

1) Machine learning methods
2) Factual models
3) Mathematical calculations

These instruments can help retrieve information expressed in quantitative, textual or multimedia structures.

Machine learning method or technique is used for the development of computational methodologies which can detect any sort of illegitimate transactions based on amount and time period of those transactions.

Mathematical calculations help in calculating the number of true frauds in the bin which are caught by the model, divided by the total number of true frauds which exists in the entire dataset.

II. LITERATURE SURVEY

Any type of fraud is a criminal activity which always results in financial or personal benefit for the scammer. It is a deliberate criminal act that is against the law, rule or policy with an aim to attain unauthorized financial benefit. Various literatures related to fraud detection in this domain have been published already and are currently available for public usage.

An extensive survey has been conducted and have disclosed that techniques employed in this domain include data mining applications, automated fraud detection, Naïve Bayes System, Hidden Markov Model, Artificial Immune System [1].

Synthetic Minority Oversampling Techniques (SMOTE) technique is used to find the fraud detection by sorting both normal as well as fraud transactions [2].

In this paper, three major ML algorithms are used: Random Forest (RF), Support Vector Machine (SVM) and Logistic Regression (LR). The results suggested that SVM shows the poorest performance in both static and incremental setup and the difference between RF and LR is slight. LR shows marginally better results in incremental setup [3].

In another paper, it is concluded that although there are a number of fraud detection systems currently being worldwide, we still need to keep a constant vigil on the methods used by the attacker as they change the means of assault every time. Genetic algorithm is preferable and also efficient in detecting credit card fraud detection [4].

Outliner detection is used which divides the detection into two parts: Supervised techniques where past known fraud cases are used to build suspicion score and secondly Unsupervised technique where there are no prior sets in which the state of the transactions is known to be fraud or legitimate [5].

Artificial Neural Network (ANN) is used for pattern recognition and prediction of future values. Like a human brain, ANN learns from the past and improves results for the future. Since training of ANN is difficult genetic algorithm is used along with it as it reduces the dataset and repeats its procedure until it finds the best solution [6].

Real time credit card fraud is detected by using predictive analytics and an API module that conveys an alert as soon as a fraudulent transaction has taken place. Also, four different

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

types of algorithms are used: Logistic Regression, Naïve Bayes, K-Nearest Neighbor and Support Vector Machine with highest accuracy rates of 74%, 83%, 72%, and 91% respectively [7].

Unconventional techniques such as hybrid data mining or complex network classification algorithms are able to perceive illegal instances in an actual online card transaction data set, based on network reconstruction algorithm that allows creating representations of the deviation of online instance from reference group have proved efficient specially on medium to small sized online transactions. Also implementing a multi-layered approach for increasing security may be helpful in reducing transaction frauds. Fraud detection is a complex process and, in this world, there is not a single system that can predict fraudulent transaction 100 percent accurately.

III. PROBLEM STATEMENT

The Fraud Detection System (FDS) problem includes modeling the past online card transactions which were labelled to be fraud. Thus, able to cross-examine and identify whether a new transaction is fraud or legit. Our aim or goal here is to detect fraudulent transaction as many as possible and minimize the incorrect fraud classifications.

IV. EXISTING SYSTEMS

A. Hidden Markov Model

HMM is embedded in online fraud detection system receives transaction details and verify whether it is legit or fraudulent. If the transaction is detected to be malicious then an alarm is raised and related bank rejects that particular transaction. Then the real owner is informed about possible card misuse.

B. Naïve Bayes System

Naïve Bayes is used in FDS because of its ability to do classification with probability and statistical methods. Naïve Bayes is really quick to respond but has quite high inaccuracy in the real world.

V. PROPOSED SYSTEM

Our project's main purpose is to develop a system which can efficiently detect online credit card fraud with the help of different methods or techniques. If a user spends significantly higher than the set transaction limit or the user's geographical location is different than the usual, then unusual pattern is detected by the system and requires re-verification or sends an alert to both the user as well as to the related bank. So based on the previous data of that user, the system recognizes unusual patterns in the payment procedure.

A. Module Description and Implementation

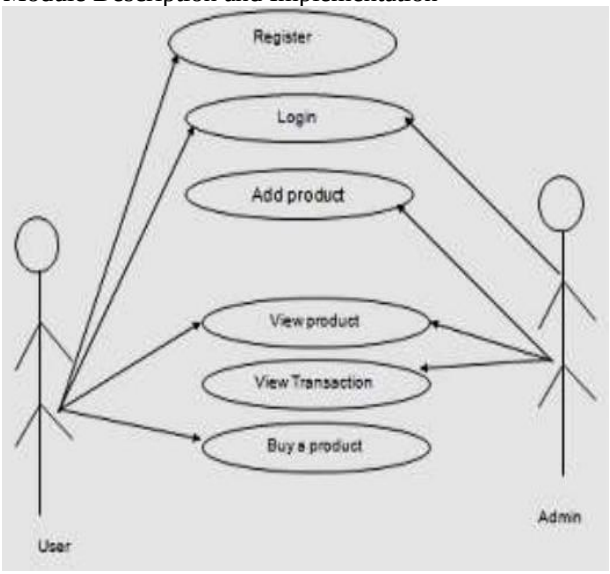

Fig. 1: Modules and interaction

1. Admin
   a. Login
   b. Add/View Products

2. User
a. Registration
b. Login
c. View product
d. Buy Product

1) Admin

Login: Admin need to login using valid login credentials in order to access the system.

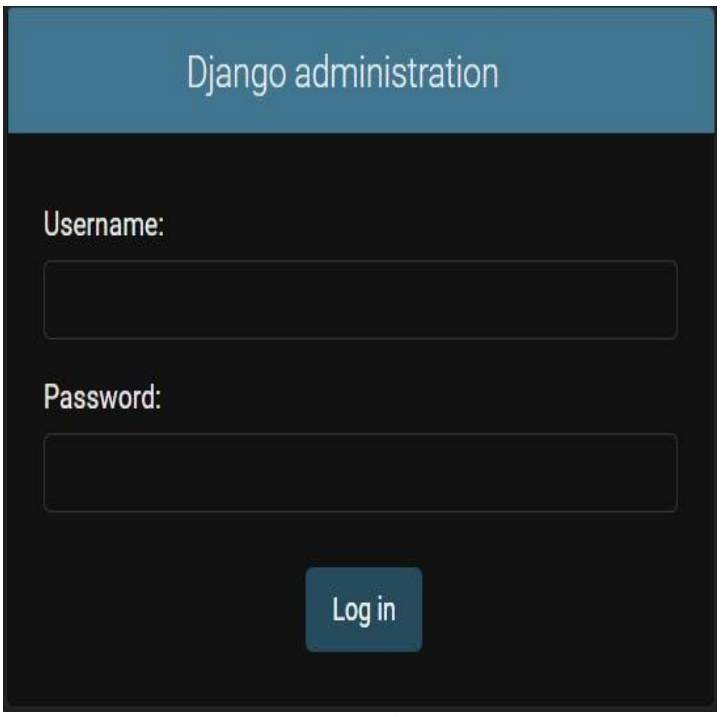

Fig 2: Login Facility for admin

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

Add/ View Products: Admin can add new product with its details into the system.

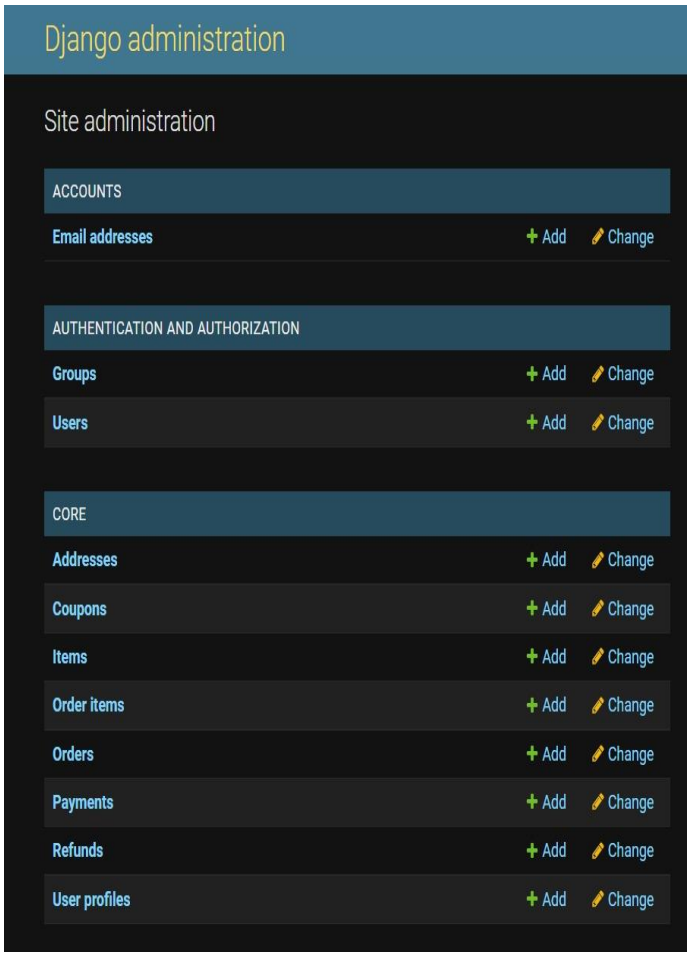

Fig 3: Modification Facility for admin

2) User:

Registration: Here, user first need to registration themselves with details to access the system.

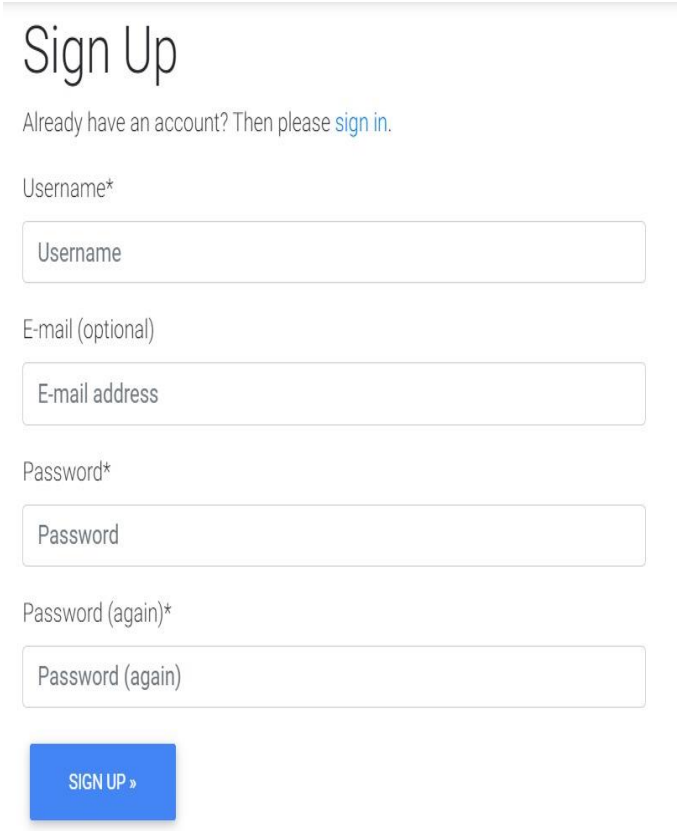

Fig 4: User Registration facility

Login: After a successful registration, user then need to login into the system by inputting their credentials into the system.

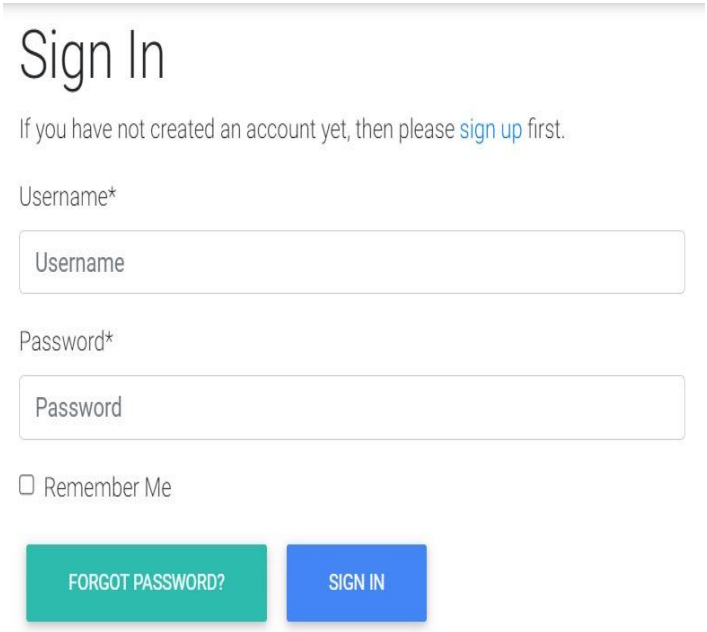

Fig 5: User Login Facility

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

View Products: User can view multiple products with its details. Interested users can purchase a product via online transaction.

Buy a Product: User can select payment mode to perform your checkout.

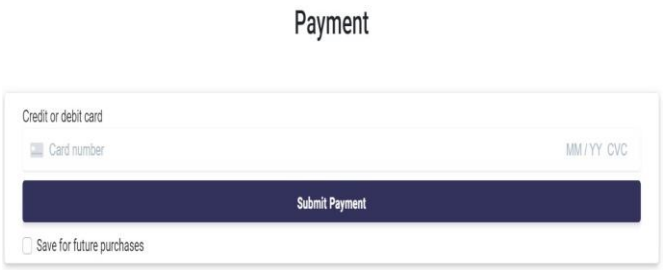

Fig 7: User Payment process screen

B. IP Geo-location against Credit Card Fraud

Credit card fraud is not just limited to the national borders, but can be carried out even on an international scale. With the emerging e-commerce businesses which provides services to international customers, scammers have now started targeting companies from anywhere in the world while also remaining hidden in the background. In most cases, the business runners only get to know about a fraud after it has already been committed. Till the time, the client complaints start coming, it is already too late to even act.

In these particular cases, the business dealers have to refund the card user which leads to a major loss in the profits. To combat this particular nuisance, new fraud detection techniques (FDS) like IP geo location has been created to help detect all sorts of unlawful transactions as soon as they occur. For instance, geodata can be used to verify all the details of a transaction made from a particular country and if any suspicious activity is noted, it instantly evaluates the matter and confirm whether the person performing the transaction is authentic or a fraud one.

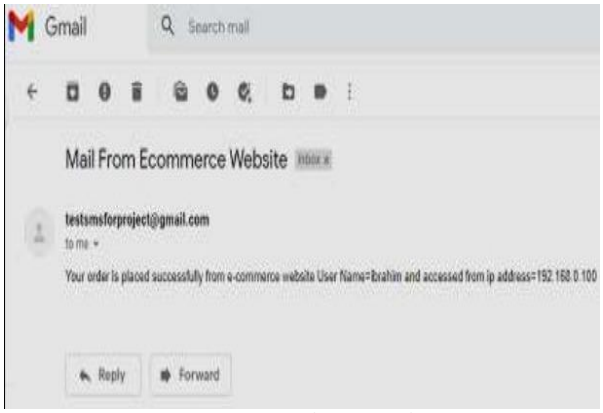

Fig 8: Ordering with Geo Location facility confirmation

VI. ALGORITHM AND FLOWCHART

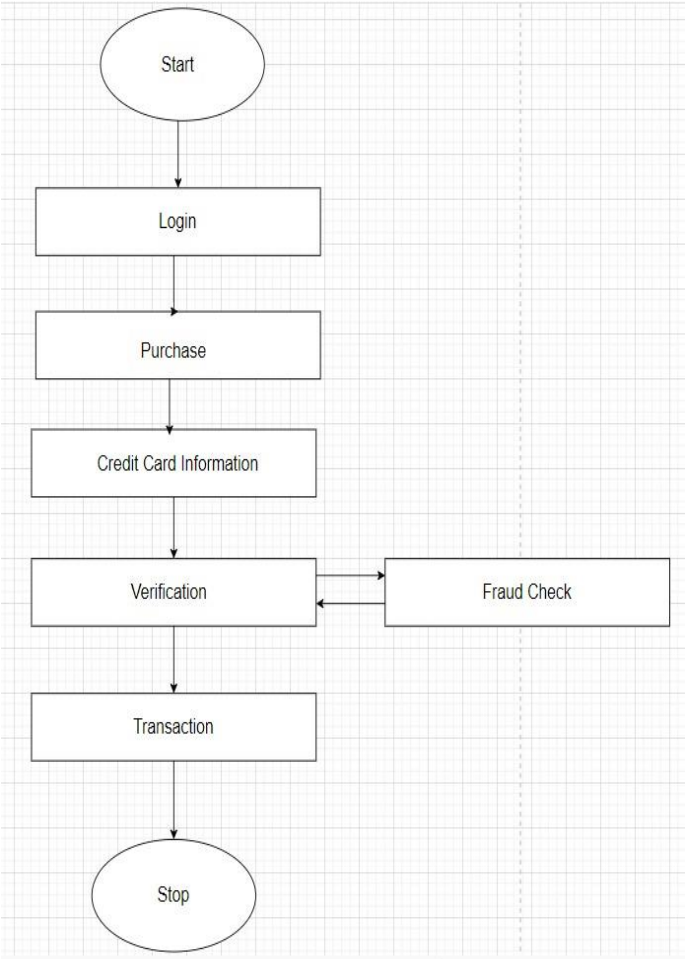

Fig 9: Flowchart of the system

Algorithm
Step 1: START
Step 2: Program initialization
Step 3: User login
Step 4: Product purchasing
Step 5: Verification card transaction limit
Step 6: If card limit > user limit
Step 7: Security questions / Alert

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 05, May-2022

Step 8: If fraud is detected, then sends location IP, OTP and username to cardholders
Step 8.1: FDS blocks transaction
Step 8.2: STOP

VII. CONCLUSION

In this paper, behavior analysis is carried out in order to detect online credit card transaction frauds in real-time. Also, the algorithm implements a multi layered security based approach for the amount of the transaction limits set by the respective user. The classification is done on the basis of the spending limit of the customer which helps in detecting whether the current transaction is genuine or fraud. Getting the geographical location of the user plays a vital role in detecting credit card fraud. The proposed system is currently useful in a small-scale website for detecting fraud and with further enhancements it could be used in a large-scale e-commerce website where thousands of transactions can happen simultaneously.

REFERENCES

[1] Prof. Radhika Mundhada1 Oz Ibrahim Ali Zahir Asan Oh2 Maneri Sohel3 Sunny Prajapati4 Momin Azhar5 " Online Transaction Fraud Detection using Python & Backlogging on ECommerce," in International Journal for Scientific Research & Development(IJSRD), Vol. 9, Issue 3, 2021, ISSN (online): 2321-0613.

[2] Aruna Kumar Joshi, Vikram Shirol, Shreekanth Jogar,Pavankumar Naik, Annapoorna Yaligar, "Credit CardFraud Detection Using Machine LearningTechniques", International Journal of ScientificResearch in Computer Science, Engineering andInformation Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 3, pp. 436-442, May-June 2020

[3] Maja Puh, Ljiljana Brkic "Detecting Credit Card Fraud Using Selected Machine Learning Algorithms" 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2019.

[4] TERUVAYI SAI CHANDU, DR. MOORAMREDDY SREEDEVI, "ONLINE TRANSACTION FRAUD DETECTION USING BACKLOGGING ON E-COMMERCE WEBSITE" Journal of Xi'an University of Architecture & Technology, Vol XII, Issue V, 2020, ISSN No:2220.

[5] Munira Ansari. Siddhesh Jadhav, Hashim Mailk, Zaiyyan Khan, "Credit Card Fraud Detection" IJERT., NREST-2021 Conference Proceedings, ISSN:2278-0181.

[6] Nikita Shirodkar, Pratiksha mandrekar,Rohit Shet Mandrekar, Rahul Sakhalkar, K.M. Chaman Kumar, Shailendra Aswale "Credit Card Fraud Detection Techniques" IEEE 2020.

[7] Anuruddha Thennakoon, Chee Bhagyani, Sasitha Premadasa, ShalithaMihiranga, Nuwan Kuruwitaarachchi "Real-time Credit Card Fraud Detection Using Machine Learning" IEEE 2019.

[8] Abrar Nadim , Ibrahim Mohammad Sayem , Aapan Mutsuddy ,Mohammad Sanaullah Chowdhury "Analysis of Machine Learning Techniques for Credit Card Fraud Detection" IEEE 2019

[9] Kit Siu, Abha Moitra, Meng Li, Cesare Tinelli, Omar Chowdhury, Daniel Prince "Architectural and Behavioral Analysis for Cyber Security" IEEE 2019

[10] Tanmay Kumar Behera , Suvansini Panigrahi "Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network" IEEE 2015