International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Online Fraud Detection on E-Commerce

Ashitosh Gole[1], Nitesh Kharatmol[2], Prof.Sonali Patil[3]

[1,2]*Student, Dept. of Computer Engineering, M.G.M. College of Engineering and Technology, Kamothe, Maharashtra, India*

[3]*Prof. Dept. of Computer Engineering, M.G.M College of Engineering and Technology, Kamothe, Maharashtra, India*

Abstract - *The frequency of online transaction has raised significant in last some of the years due to popularization of e-commerce. We also noticed the significantly increasing the online fraud cases, resulting in billions of dollars losses each year worldwide. Hence it is important and necessary to developed and apply techniques that can assist in fraud detection. Which motivate our research. This work aims to apply and evaluate the computational intelligence techniques to identify and detect the fraud and make more secure web payment gateway and another online payment system. In order to evaluate the techniques, we apply and evaluate them in an actual data set of the most popular Brazilian Electronic payment System. Our project shows good performance in fraud detection and it helps to gain 43% of economics matric.*

***Key Words*: E-Commerce, Online payment, E-Business, dataset, payment gateway.**

1. INTRODUCTION

Today due to rapid growth online transaction is grown day by day. The mode of payment is done by credit card or online payment method. The also credit card and Gpay users are increasing day by day. It was reported that there are almost 430 million credit and debit card users across whole Europe. As the number of credit/debit card/Gpay users increasing, the fraudulent users are also increasing.

The user has to inform the details while making payment. In this type, if fraudulent user wants to access his/her card or any of bank related details then he just needs to steal that details. In virtual card, the fraudulent user needs to know the information about details information about credit card such as, CVV no, Secure code, Credit card number. Therefore, the secure payment gateway is needed to identify the user and to verify that the user is legal or attacker. The most useful and appropriate technique used for fraud detection is Behavior and Location Analysis (BLA).

1.1 Online Fraud

Types of online fraud are called phishing and spoofing. Phishing is the process of collecting your personal information through e-mails or websites. This information can include usernames, password, credit card details, social security numbers, etc. Often times the e-mails directly connect you to a website where you can update your personal information. Because these sites often look "Official" they hope you'll be tricked into disclosing valuable information that you normally would not reveal. This often results is identify the theft and financial loss. Spyware and Viruses are both malicious programs that are loaded on your computer without your knowledge. The purpose of these programs uses to capture or destroy information, to ruin computer performance or to overload you with advertising. Viruses can spread by infecting computers and then it replicates. Spyware disguises itself as a legitimate application and embeds itself into your computer where it they monitor your activity and collects information.

1.2 Types of Online Fraud

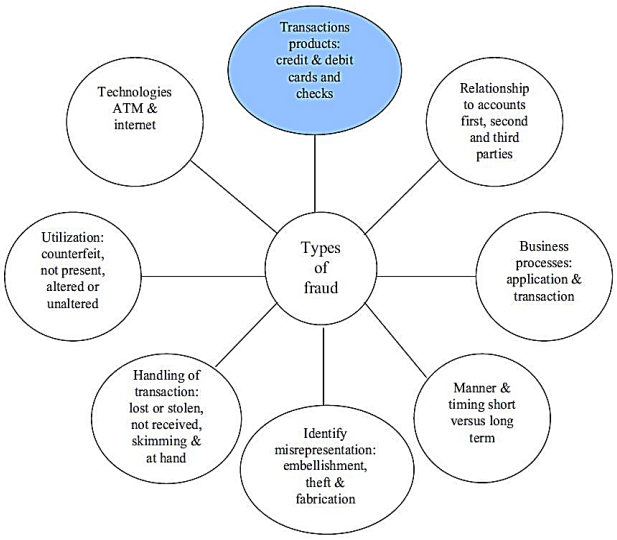

Fig -1: Types of Fraud

Online Payment Account Generation

There was open to online account they need the Users credit card details to open the account, need to enter the CVV, Card number and most important thing have an OTP (one time password).

1.3 RANDOM FOREST

Random forest algorithm is useful for detect the unwanted activity faster and it help to sort out the thing in the object efficiently to help the things. the method is useful for find unwanted or suspicious activity in multiple class object. In this it detects the one fraudulent user from many of the user.

2. SCOPE and OBJECTIVE

The system prevents on fraudulent users from misusing the details of the credit-card of the genuine users for their personal gain. The spending habits of the owner is detecting the fraud. As the fake user might not be aware of the spending habits of the owner, there will be an irregularity in spending pattern, which the system will detect. The owner is immediately alerted about the attempted fraud and the transaction is blocked performed by attacker. Thus, the system protects legitimate users from financial loss. The system helps making electronic payment safer and more reliable. The principles in the proposed system can also adopted and implemented in other electronic payment services such as online banking facility and payment gateways.

- Creating an application to detect fraud Credit Cards.
- Implementing Hidden Markov model.
- Creating database containing all relevant information of Customer.
- Providing security to the customers at the time of transaction.

3. EXISTING SYSTEM

Credit card frauds are increasing rapidly nowadays because of fraud financial loss is increasing drastically. Billions of amounts is lost every year due to fraud. To analyze the fraud there is lack of research. Many machine learning algorithms are implemented to detect credit card fraud. Logistic Regression, Decision Tree Model, Artificial Neural Network, Gradient Boosting Algorithm and Hybrid algorithms are applied. The objective of the project is to detect credit card fraud detection by implementing machine learning algorithm with relevance to time and amount of transaction.

4. PROPOSED SYSTEM

The aim of proposed system is to develop a website which has capability to restrict and block the transaction performing by attacker from genuine user's credit card details. The system is developed for the transactions higher than the customers current transaction limit. As we seen existing system detects the fraud after fraud has been occurred i.e., based on customers complained. Proposed system tries to detect fraudulent transaction before transaction succeed.

In proposed system, while registration we take required information from user which is efficient to detect fraudulent user activity,

- In proposed system, I present a Behavior and Location Analysis (BLA).
- Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit.
- Card transaction processing sequence by the stochastic process of a BLA.
- The details of items purchased Individual transactions are usually not known to any Fraud Detection System (FDS) running at the bank that issues credit cards to the cardholders.
- Hence, I feel that BLA is an ideal choice for addressing this problem.
- Another important advantage of the BLA - based approach is a drastic reduction in the number of Fail Pass transactions identified as malicious by an FDS although they are actually genuine.
- An FDS runs at a credit card issuing bank. Each incoming transaction is submitted toward the FDS for verification.
- FDS receives the card details and the value of purchase to verify, whether the transaction is genuine or fake.
- The types of goods that are bought in that transaction are not known to the FDS.
- It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc.
- If the FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

The credit card fraud detection feature use user behavior and location scanning to check for unusual patterns. These patterns include user characteristics such as users spending patterns as well as usual user geographic locations to verify his identity. If any unusual pattern is detected, the system requires re-verification of the user.

The system analyzes user credit card data for various characteristics. These characteristics include user country, usual spending procedures. Based upon previous data of user the system recognizes unusual patterns in the payment procedure. So now the system requires the user to login again or even block the user for more than 3 invalid attempts.

5. ALGORITHM

Step1: - Initial state
This state is indicating the first stage of payment process for e.g. of opening payment gateway window
Step 2: - If find out some suspicious activity else go to **step 5**
If user cross its payment limit or it may enter incorrect details then it calls for the security check. The dataset consists of credit card transactions whose features are the product of PCA analysis and thus we don't know what they represent except from the 'Amount', 'Time' and 'Class' ones. 'Amount' is the price of each transaction, 'Time' is the <<seconds elapsed between each transaction and the first

transaction>> and 'Class' represents a **fraud transaction** when its value equals **1** and a **valid transaction** when its value equals **0**.

Step 3: - It ask the ask the user for security question.
Those question and answer accept at the login activity

Step 4: - If user fails to answer correctly then it informs or alert the bank system about the activity happens.

Step 5:- else it corrects then it goes and complete the transaction

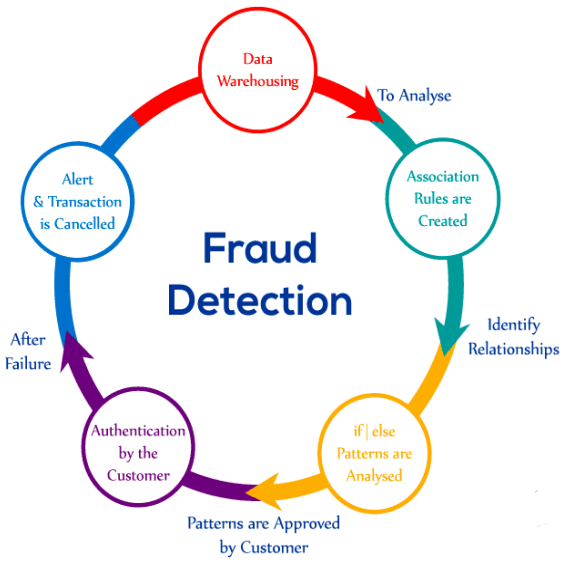

Fig -2: Flow of Fraud Detection

6. WORK FLOW

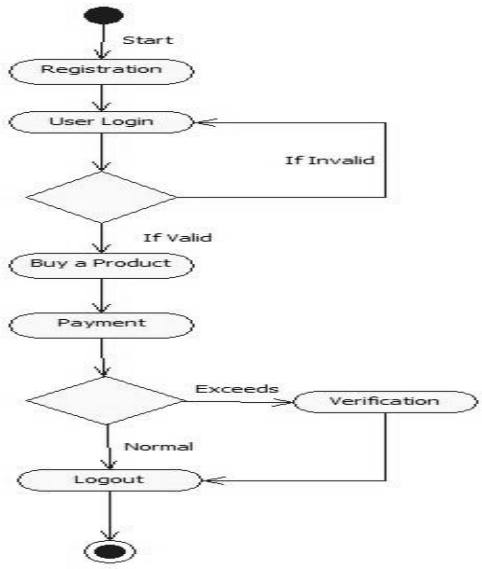

Fig -3: Workflow

7. PROJECT IMPLEMENTATION AND TEHCNOLOGIES

The Project is designed and developed in Django Framework. We used Django Framework for coding of the project. Created and maintained all databases into MySQL Server, in that we create tables, write query for store data or record of project.

- **Hardware Requirement**
  - Processor –Core i3
  - Hard Disk – 160 GB
  - Memory – 1GB RAM
  - Monitor
- **Software Requirement**
  - Windows 7 or higher
  - Python
  - Django framework
- Database
  - MySQL

8. CONCLUSION

Credit card fraud is a criminal dishonesty. In this paper describe different types of fraud, such as bankruptcy fraud, counterfeit fraud, theft fraud, application fraud and behavioral fraud, and discussed measures to detect them. It has included pair-wise matching, decision trees, clustering techniques, neural networks, and genetic algorithms. Yet, the unprofessional fraudster is unlikely to operate on the scale of the professional frauds ter and the costs to the bank of their detection may be uneconomic. The bank would be faced with an ethical dilemma. Should they need try to detect such fraudulent cases or should they act in shareholder interests and avoid uneconomic costs? The next step in research program, the focus will be upon the implementation of a 'suspicious' scorecard on a real data-set and its evaluation. The main tasks is to build scoring models to predict fraudulent behavior, taking into account the fields of behavior that relate to different types of fraud identified in this paper, and to evaluate the associated ethical implications. The plan is to take one of the European countries, probably Germany, and then to extend the research to other EU countries.

ACKNOWLEDGEMENT

Working on the project on Online Fraud Detection was a source of immense knowledge to us. However, this would not have been possible without the equal support of all members. I sincerely express my deep sense of gratitude to our Asst.Prof. Sonali patil, for her valuable guidance, continuous encouragement and support whenever required and timely help given to us throughout the course of this work

REFERENCES

[1] CLIFTON PHUA1, VINCENT LEE1, KATE SMITH1 & ROSS GAYLER2 "A Comprehensive Survey of Data Mining-based Fraud Detection Research" published by School of Business Systems, Faculty of Information Technology, Monash University,

[2] "Survey Paper on Credit Card Fraud Detection by Suman", Research Scholar, GJUS&T Hisar HCE, Sonepat published by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 3, March 2014

[3] "Research on Credit Card Fraud Detection Model Based on Distance Sum –by Wen-Fang YU and Na Wang" published by 2009 International Joint Conference on Artificial Intelligence

[4] "Credit Card Fraud Detection through Parenclitic Network Analysis-By Massimiliano Zanin, Miguel Romance, Regino Criado, and SantiagoMoral" published by Hindawi Complexity Volume 2018,

[5] "Credit Card Fraud Detection: A Realistic Modelling and a Novel Learning Strategy" published by IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, VOL. 29, NO. 8, AUGUST 2018

[6] "Credit Card Fraud Detection Using Machine Learning Models and Collating Machine Learning Models by Navanshu Khare and Saad Yunus Sait" published by International Journal of Pure and Applied Mathematics, Volume 118 No. 20, 2018.