Online Transaction And Fraud Detection

Dr. G. Kalpana[1], V.Raja[2]
[1,]Associate Professor, Dept of Computer Science
[2]Assistant professor, Dept of Computer Science
[1, 2] SRM Institute of Science and Technology, Kattankulathur, Chennai – 63

Abstract*-This is a mechanism which is used to control and manage the usage of credit card and debit card details of the genuine users. This system provides validation on transactions with higher limits under current usage limit. We manage to stop or drop a transaction before it is processed by a fraud. During this initial process we take the required details and Information of the particular user and store within a database. We provide a method of identifying the location of the access and behavior of the transaction. The information or details of the items purchased are usually not known by the fraud detection systems in the bank from where the credit or debit cards are provided therefore we develop a location and behavior analysis module. The benefit of this method is that it reduces the wrong information provided by the bank or fraud detection system regarding a particular transaction which is identified as malicious or fake although it is genuine or true.*

Fraud detection system is usually preferred by credit cards issuers. Each transaction is submitted for verification and validation of the data the provided by the user during the transaction. Fraud detection system may receive the details of the card and the transaction history to analyze and verify the data, whether the transaction is a fraudulent or genuine. The products or goods purchased by the user are not known by the respective bank where transaction is processed. Therefore bank declined the transaction if fraud detection system confirms the transaction to be fraud. The spending methods and the geo-location are being tracked periodically during every transaction where any such intruder pattern is located the system requires re-verification with the data which is stored within the database, If the system transaction procedure recognizes unusual forms. The system will block the user after 3 wrong attempts.

Keywords- fraud detection, transactions, intruder, malicious

I. INTRODUCTION

In this modern world online transaction is growing day by day due to the rapid growth of commerce, Online Trading, and etc. Mostly the payments of these transactions are done by payment cards like credit or debit. We have a statistical report which proves that more than 540 million credit and debit cards are used among the people for online transactions [1][2]. Therefore the number of users increase simultaneously the fraud activities are also increased. Mostly payment cards like credit or debit are generally classified into two categories such as

i. Virtual Card,
ii. Physical Card.

When a physical card is used, the user must show the card in-person [3-6] where the transaction is made therefore if the fraudulent wants to know the card details he/she needs to steal the physical card from the user. but in a virtual card, the person who wants to steal the data needs information about card such as card verification value number, high security password, validity of the card & the 16 digit card number to identify the provider[5][6] . So naturally we need a secure platform or gateway to ensure that the card is accessed only by the genuine users and not the fraudulent. Therefore we have developed a technique to overcome this issue with some kind of security measure known as Behaviour and location analysis method.

1.2 LITERATURE SURVEY

1.2.1 TRANSACTION FRAUD DETECTION

Due to the growth of modern technology, the mode of payment of individual has changed significantly. The use of Online Payment mode such as Online Banking, Debit Card, Credit Card etc. has become popular and is becoming important in day today activities because it allows bank customers to purchase goods and services from the shopping websites or from the market. Fraud deals with cases that happen due to criminal purpose which are difficult to identify[1].

Fraud can be mainly divided into two types:

i. Offline Fraud:

Most of the offline fraud incidents occur due to the steal of purse/wallet that contains important documents. Documents such as Driving License, ID card etc. contains crucial information such as name, date of birth, transaction slips etc [3].

ii. Online Fraud:

Online fraud occurs when fraudster present their website as a genuine website in order to obtain crucial personal data of a customer and perform illegal transactions on such customer account. Credit card is also one of the most illegal types of fraud. Credit Card is aplastic card i.e. issued to customers of a bank as one of the mode of payment [7]. It allows cardholders to purchase goods and services from the shopping websites or from the market. Credit Card Fraud is defined as, when an individual uses another individual credit card for personal use while the owner of the card as well as the card issuer are not aware of the thing that the card is being used. If credential information of a customer has stolen and uses for online shopping, the card holder acknowledges transaction details after the fraud has been committed and then customer inquire the bank for transaction. There is no such process that can prevent fraudulent transaction at the time of happening. So there is a need of such interface that prevents from online transactions.

1.2.2 SECURITY MECHANISM TO PREVENT FROM FRAUD

These are the existing security mechanism that helps to prevent from fraudulent transactions:

a) Address Verification Service (AVS):

In this technique it matches the cardholder billing address and shipping address and identifies whether the cardholder has purchased product on this address. However, this technique contains some weaknesses i.e. the address information is available online; the banker feels boring to check record of every customer to prevent from fraudulent transaction; it cannot check the entire informational card.

b) Fraud Rates:

This technology checks for recognized patterns i.e. used by the fraudster to commit the fraud. The advantage that it is easy to configure and understand, but the disadvantage fraudster changes their pattern changes at regular interval [8].

c) Relocation:

This technology identifies the customer geographic location by identifying its IP addresses.

d) Chip & Pin:

A PIN is a 4 digit unique and secret number that customer has to enter before doing transaction by ATM/Debit Card/Credit Card [5]. The 4 digit pin is used to identify whether the customer is genuine or not.

e) 3D-Secure:

This technology works on the principle of authenticating the user password with the password i.e. stored in the database [6]. The main advantage of this system is that fraudster needs a user’s password to perform the transaction.

f) One Time Password:

The random number is generated at server side and is send to the customer‟s mobile phone through the help of the web services to ensure that the correct user is performing the transaction at that instant of time. The user has to enter the same password forgetting the authorization from the bank side [7].

g) Fraud Detection System:

All the information about credit card (Like Credit card number, credit card CVV number, credit card Expiry month and year, name on credit card etc.) will be checked with credit card database. If User entered database is correct then it will ask Personal Identity number (PIN).

After matching of Personal Identity number (PIN) with database and account balance of user’s credit card is more than the purchase amount, the fraud checking module will be activated [11]. The verification of all data will be checked before the first page load of credit card fraud detection system [9].If user credit card has less than 10 transactions then it will directly ask to provide personal information to do the transaction [12]. Once database of 10 transactions will be developed, then fraud detection system will start to work. By using this observation, determine users spending profile. The purchase amount will be checked with spending profile of user [13] . By transition probabilistic calculation based on HMM, it concludes whether the transaction is real or fraud [1][8][10]. If transaction may be concluded as fraudulent transaction then user must enter security information. This information is related with credit card (like account number, security question and answer which are provided at the time of registration). If transaction will not be fraudulent then it will direct to give permission for transaction

1.3 PROBLEM OBJECTIVE

To overcome the stated problem between the payment gateway under various E-commerce websites and the customer to rectify the genuine users from Fraudulent

Here we present a Behavior and Location Analysis (BLA) mechanism. User spending patterns and geographical location is used to verify the identity. If any unusual pattern is detected, the system requires re-verification. Based upon previous data of that user the system recognizes unusual patterns in the payment procedure. System will block the user after 3 invalid attempts.

1.4 PROBLEM DEFNITION:

Here the problem states that every online transactions nowadays are pushed towards several security authentications for the verification and validation of authenticity of the users. The details of items purchased in Individual transactions are usually not known to any Fraud Detection System (FDS) running at the bank that issues credit cards to the cardholders. Where types of goods that are bought in those transactions are not logged into the FDS_db. Therefore Bank declines the transaction if FDS confirms the transaction to be fraud.

1.5PROPOSED SYSTEM:

The proposed system is completely based on a website, which is developed with a functionality to block or restrict a particular transaction which is initiated by the hackers or attackers by using the credentials of a genuine user card details. The mechanism is generally developed for payments or transactions higher than the current usage limit.
In the existing system we saw that the fraud detection was initiated only after the transaction is been occurred.

Therefore the proposed system manages to find or detect the fraudulent activities before the transaction is succeeded.

In the proposed system we try to gather the information’s and details which is required to find the fraudulent activities.

- Provide a Behavior and Location Analysis mechanism (BLA).
- It does not require any fraud fingerprints but still its able to find the frauds by considering the users spending pattern.
- Transaction using cards are processed by stochastic processes in Behavior and location Analysis
- The bank who provides payment cards to the user never knows about the individual spending patterns of the user and the products which the user intended to purchase.
- Therefore behavior and location Access method is the best option to manage.
- The best service provided by the BLA method is that it is capable of identifying the false positive transactions although it is genuine from the user.
- FDS receives card details and buyer's value to check whether the transaction is true or not.
- This method seeks to find any extraordinary transactions based on the cost of the cardholder, shipping address and billing address.
- If the fraudulent detection method ensures fraud's transaction, it raises the warning, and the bank that the transaction has refused.

The fraudulent detection system verifies the transaction for unusual forms, in which methods are user identifiers to verify the identity of user ID methods and unique user geo-locations. If any extraordinary method is detected, the system needs verification or data validation.

Fraud detection system analyzes user credit card data for various attributes. These attributes are user country and regular cost practices. The system recognizes abnormal patterns in payment mode, based on that user's previous data. So now you have to log into the system again or the user must have 3 incorrect errors.

1.6 RESULTS AND DISCUSSIONS

1.6.1 ADMIN MODULE

- **Login:** Admin must sign in with valid login credentials to access the system.
- **Products Add:** Admin can add new product to its detailson the system.
- **Transactions visual:** System Administration allows access to all transactions made by registered users.

1.6.2 USER MODULE

- Registration: Here, you need to register the details first to get user access.
- Sign: After a successful registration, the user must log in to the system to enter their credentials.
- View products: User can see many products in its details. &Interested users can buy a product through online transaction.
- Buy a product: card number, cvv By selecting card details such as code, expiration date and holders name, you can select user activity methods.

- Display transaction: The list of all transactions will be shown to the user.

1.4 CONCLUSION & FUTUREENHANCEMENT

Clearly, credit card fraud is a criminal dishonest act. This article has reviewed the recent findings in the credit card industry. The sheet has found a variety of frauds, such as bankruptcy fraud, counterfeit fraud, theft fraud, utility fraud and behavior fraud, and discussing measures to find them. Such activities include couples matching, ending trees, masonry techniques, neural networks, and genetic codes. From a protocol perspective, banks and credit card companies have argued that all fraud cases are trying to find. Nonetheless, the fraudulent bank's expenses may be uninterrupted as it does not know the amount of professional fraud. The bank will then face a protocol dispute. Do they want to find such fraudulent cases or to act in the interests of shareholders and avoid economic spending? The next step of this research program will focus on implementing a 'doubtful' score in a genuine data set and its assessment. The main tasks are to create scores to evaluate fraudulent behavior, to assess the various types of credit card fraud identified in this paper and to assess relevant regulatory implications.

This program is one of the EU countries, perhaps Germany, and the expansion of research to other EU countries.

REFERENCES

[1] The State of Threat Detection'. Fidelis Cybersecurity, 3 Dec 2018. Accessed Dec 2018.

[2] brahim H, Ghandour M, Dimitrova M, Ilinca A, Peron J. Integration of wind energy into electricity system: technical challenges and actual solutions. Energy Proceedia 2011;6:815–24.

[3] Hansen AD, Hansen LH. Wind turbine concept market penetration over 10Years (1995–2004). Wind Energy 2007;10(1):81–97.

[4] Ramey DG, Henderson M. Overview of a special publication on transmission system application requirements for FACTs controllers. Power Energy Society General Meeting 2007:1–5

[5] Muller S, Deicke M, De Doncker Rik W. Doubly-Fed Induction Generatorsystem for wind turbines. IEEE IndustApplicat Mag 2002.

[6] Hhughes FM, Anaya-Lara O, Jenkins N, Strbac G. A power system stabilizer forDFIG-based wind generation. IEEE Trans Power Syst 2006;21(2):763–72.

[7] Rahman SA, Verma RK, Litzenberger WH. Bibliography of FACTs applicationsfor grid integration of Wind and PV solar power systems: 1995–2010. In: IEEEworking group report, Power and energy society general meeting. p. 1–17.

[8] Thukaram D, Abraham L. Selection of static VAR compensator location and sizefor system voltage stability improvement. Electric Power System Res 2000;54(2):139–50.

[9] Lund T, Sorensen P, Eek J. Reactive power capability of a wind turbine withdoubly fed induction generator. Wind Energy 2007;10:379–94.

[10] Pali BS, Bhowmick S, Kumar N. Power flow models of static VAR compensator.In: IEEE Fifth Power India conference. p. 1–5.

[11] Modelling of SVC in Power Systems Studies. ABB Power Systems, Sweden.

[12] The ABB Static VAR Compensator, ABB Utilities AB Power Systems, Sweden.

[13] Erinmez IA. Static VAR compensators. CIGRE Working Group,.Task force no. 2on SVC. 1986;38(1).