Review on Fraud Detection in Electronic Payment Gateway

Miss. Akshada K. Dhakade[1], Prof. K.K.Chhajed[2], Prof. A.S.Kapse[3]

[1]Miss.Akshada K. Dhakade, P.R.Pote College Of Engineering, Maharashtra, India.
[2] Prof. K. K. Chhajed, Assistant Professor Department of Computer Science and Engineering, P.R.Pote College Of Engineering, Maharashtra, India.
[3]Prof. A. S. Kapse, Assistant Professor Department of Computer Science and Engineering, P.R.Patil College Of Engineering, Maharashtra, India.

---***---

Abstract - *Due to rapid advancement in the electronic commerce technology the use of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for online as well as regular purchase. Fraud is a major problem in electronic payment systems. Credit Card fraud happens when card are lost or stolen and when mail or OTP (One Time Password) is delivered from the intended recipient and taken by criminals. Consequently, Fraud detection is becoming an important issue for research. Reducing fraud is a complex process which includes the knowledge scientific areas and demands a multidisciplinary approach. Encryption is a way to hide and transport sensitive information. Credit card numbers for online transactions, social security numbers in employee databases, and other personal and financial information all need to be encrypted. System reduces fraud through OTP and Secret Code. This secret code stored in encryption format so unauthorized user cannot use this secret code.*

Key Words: Payment Gateway, E-commerce, Credit Card, Secret Code, OTP.

INTRODUCTION

Payments using credit cards have increased in recent years. It may be used in online or in regular shopping. Now-a-days credit card payments are necessary and convenient to use. Banking system provides e-cash, e commerce and e-services improving for online transaction. Credit card is one of the most conventional ways of online transaction. In case of risk of fraud transaction using credit card has also been increasing. Due to a rapid advancement in the electronic commerce technology, the use of credit cards has increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of credit card fraud also rising [4].

Financial fraud is increasing significantly with the development of modern technology and the global superhighways of communication, resulting in the loss of billions of dollars worldwide each year. The fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. The concept of paying for goods and services electronically is not a new one. Since late 1970 and early 1980, a range of Methods has been initiated to accept payment to be resulted across a computer network. After a period of rapid expansion, 1.5 billion populations have internet access globally as of 2008.

The e-commerce began at the beginning of the year 1997, an enormous selection of diverse payment techniques developed by the researched some of these were instigated some of these were instigated on the market and unsuccessful to arrive at a critical mass. The e-commerce is a process of value exchange in electronic e-commerce; where the amount is transferred online on internet, other computer network. Normally existing fraud detection system for online banking will detect the fraudulent transaction after completion of the transaction.

Credit Card- based purchases can be categorized into two types:
1. Physical Card: In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card.
2. Virtual Card: In the second kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the "usual" spending patterns.

1.1 Fraud Techniques

Various types of fraud techniques are as follows:

A. Site Cloning: In site cloning the fraudster clone an entire site or just the payment page of the site where customer make a payment. Customer feels that they are viewing the real site. The customer handover a credit card detail to the fraudster and then fraudster sends the customer a transaction receipt via email as real site. Thus fraudsters have all detail of customer credit card so they can commit fraud without customer's awareness.

B. Stolen / Lost Credit Card: When customer card is lost or stolen by fraudster he gets all the information of the cardholder in the easiest way without investing any modern technology. It is difficult form of credit card fraud to detect.

C. Skimming: Skimming is one of the popular forms of credit card fraud. It is a process where the actual data on a card is electronically copied to another. It is very difficult for cardholder to identify this type of fraud.

D. Credit Card Generator: In credit card generator the computer program generates the valid credit card number and expiry gate. This generator creates a valid credit card highly reliable that it looks as the valid credit card number only and are also available for free download off the internet.

E. Phishing: In phishing the fraudster sends lots of false email to card holder. The e-mail looks like they came from the website where the customer trust for example customers bank. The email asks the customer to provide personal information like credit card number. With the help of these details fraudster commits crime.

F. Internal Fraud: The employee or owner access customer's detail. The steals the customer's personal information to commit crime or pass on the information about cardholder to fraudster for money [10].

2. LITERATURE SURVEY

2.1 Payment Gateway: An Overview

Payment Gateways play an integral role in facilitating ecommerce. Without the creation of a secure method for moving sensitive data the ability to conduct non face to face commerce could not have happened. Today there are many gateway providers serving up diverse solutions. But before 1996 there was no option. We wanted to understand the history and genesis of the payment gateway.

A Payment Gateway is a merchant service provided by an e-commerce application service provider that authorizes credit card or direct payment processing for e-businesses, online retailers, bricks and clicks, or traditional brick mortar. A payment gateway facilitates a payment transaction by the transfer of information between a payment portal (such as a website, mobile phone or interactive voice response service) and the front end processor or acquiring bank [5].

2.2 Fraud : An Overview

The Association of Certified Fraud Examiners (ACFE) defined fraud as "the use of one's occupation for personal enrichment through the deliberate misuse or application of the employing organization's resources or assets." In the technological systems, fraudulent activities have occurred in many areas of daily life such as telecommunication networks, mobile communications, online banking, and E-commerce. Fraud detection involves identifying fraud as quickly as possible once it has been perpetrated. Fraud detection methods are continuously developed to defend criminals in adapting to their strategies. The development of new fraud detection methods is made more difficult due to the severe limitation of the exchange of ideas in fraud detection at present; fraud detection has been implemented by a number of methods such as data mining, statistics, and artificial intelligence. Fraud is discovered from anomalies in data and patterns.

2.3 Related Work

The technology for detecting credit card frauds is advancing at a rapid pace. This has attracted much researchers attention recently due to increase in credit card fraud. Some of the popular techniques employed by Issuing and Acquiring banks these days are; rule based systems, neural networks, data mining, grid based hidden Markov Model, etc.

Protecting transaction data and cardholder information has been the main driver in introducing smart cards worldwide and for the adoption of the EMV standard. Data authentication in EMV checks whether the card is genuine using the Card Authentication Methods (CAM) supported by the chip, all of which rely on public key cryptography. EMV has dramatically reduced fraud where it has been deployed, but counterfeiting is still a risk.

Ashlesha Bhingarde, Avnish Bangar, Krutika Gupta, Snigdha Karambe [9] have proposed Credit Card Fraud Detection using Hidden Markov Model. Hidden Markov Model is the statistical tools for engineer and scientists to solve various problems. Hidden Markov Model is a perfect solution for addressing detection of fraud transaction through credit card. One more important benefit of the HMM-based approach is an extreme decrease in the number of False Positives transactions recognized as malicious by a fraud detection system even though they are really genuine. In this prediction process, HMM consider mainly three price value ranges such as:

1) Low (l),
2) Medium (m) and,
3) High (h).

First, it will be required to find out transaction amount belongs to a particular category either it will be in low, medium, or high ranges [8] [9].

V. Dheepa and R. Dhanapal developed [4] credit card fraud detection using Support Vector Machines. Support Vector Machines are employed and efficient feature extraction method also adopted. If any discrepancies occur in the behaviours transaction pattern then it is predicted as suspicious and taken for further consideration to find the frauds.

Behaviour based fraud detection model means that the data use in the model are from the transactional behaviour of cardholder directly or derived from them. Each person may have a different spending behaviour pattern. Most of the existing fraud detection methods use the behaviour pattern as measure to find the destruction in the transactions. Based on the spending pattern the customer's usual activities such as transaction amount, billing address etc. are learned. Some of the count measures to suspect the behaviours are the variation of billing address and shipping address, maximum amount of purchase, large transaction done far away from the living place etc. Like that the behaviours deviate from the normal ones are suspected and taken for further consideration [4].

Support vector machine is a method used in pattern recognition and classification. It is a classifier to predict or classify patterns into two categories; fraudulent or non-fraudulent. It is well suited for binary classifications. As any artificial intelligence tool, it has to be trained to obtain a learned model. SVM has been used in many classification pattern recognition problems such as text categorization, bioinformatics and face detection. SVM is correlated to and having the basics of non-parametric applied statistics, neural networks and machine learning.

Twinkle Patel, Ms. Ompriya Kale[10] developed credit card fraud detection using Hidden Morkov Model. HMM is used along with HOTP to make HMM more secured as we have seen above HMM [9] needs training and during training some transactions are involved and fraud is not detected during training but it is detected after training so HOTP is used for secured approach in HMM so make initial transaction secure by sending one time password i.e. security code to clients mobile if the security code entered by client is correct then only transaction is done successfully else transaction is not allowed to progress. But once the HMM is trained and ready for detection client does not need to enter any security code unless HMM detects the transaction is above threshold value. If the transaction is above threshold value security code is send to mobile and client need to enter that security code then only transaction is done successfully else transaction is not allowed to progress [10].

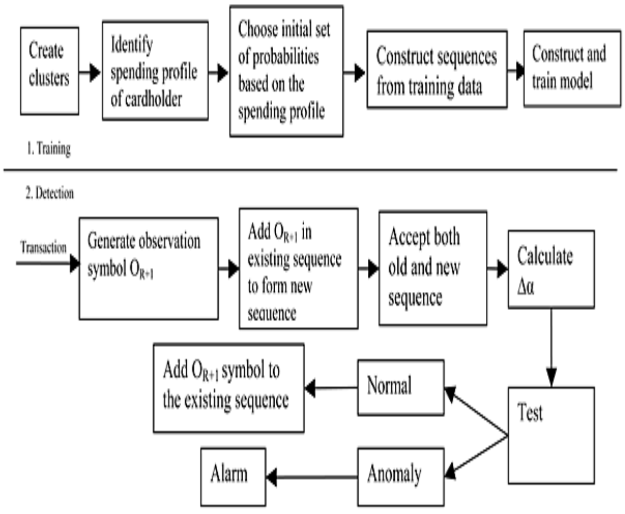
Create clusters
Identify spending profile of cardholder
Choose initial set of probabilities based on the spending profile
Construct sequences from training data
Construct and train model
1. Training
2. Detection
Transaction
Generate observation symbol O_{R+1}
Add O_{R+1} in existing sequence to form new sequence
Accept both old and new sequence
Calculate $\Delta\alpha$
Test
Normal
Anomaly
Add O_{R+1} symbol to the existing sequence
Alarm

Fig.1 Process flow of Credit Card Fraud Detection System using HMM

As shown in Fig. 2 there are two phases of HMM. In training phase card holder transaction amount is converted in observation symbols i.e. low medium or high and form sequences from them. After the sequence is formed threshold is calculated from the sequence of amount.

In the detection phase client enters amount and form an initial sequence of symbol. Let O1, O2, O3………..OR be such sequence of length R up to time t. This sequence is the input to HMM and from that we compute the threshold of acceptance α1. Let OR+1 be a symbol of new transaction at time t+1.now with new transaction we generate a new sequence O2, O3,………..OR ,OR+1. We input these sequence in HMM and calculate the new threshold of acceptance if amount is less than threshold than amount is added in new sequence else the it is detected as anomaly

V.Priyadharshini, and G.Adiline Macriga [11] Credit Card Fraud Detection using Finger Print Recognition. The main objective of this proposed method is to achieve resilience by adding two new, real time, data mining based layers to complement the two existing non data mining layers proposed system utilizes real time data mining- based security layers (CD and SD) for identity crime detection. The first new layer is Communal Detection (CD): the white list-oriented approach on a fixed set of attributes. To complement and strengthen CD, the second new layer is Spike Detection (SD): the attribute-oriented approach on a variable-size set of attributes. The CD and SD layers are continuously updated. Data are traditionally based on a binary representation in which discrete information is assumed (even in continuous data, range representations are possible) and so the operations involve "modifying" bits without concern for any underlying semantics. In dealing with text data, representing the linguistic knowledge is an important issue in which traditional binary coding is insufficient, and so new representation schemes should be investigated.

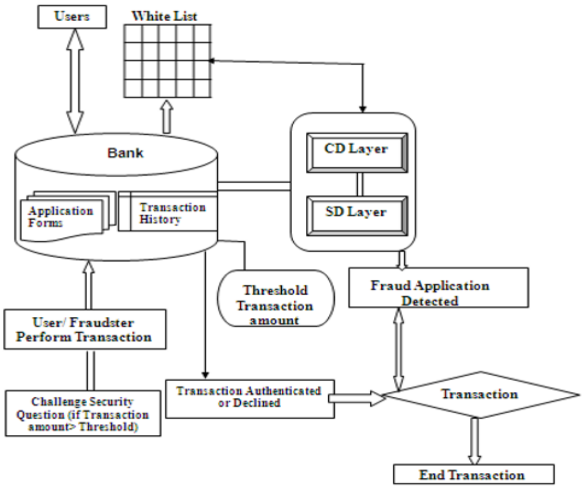
Users
White List
Bank
Application Forms
Transaction History
CD Layer
SD Layer
Threshold Transaction amount
Fraud Application Detected
User/ Fraudster Perform Transaction
Challenge Security Question (if Transaction amount> Threshold)
Transaction Authenticated or Declined
Transaction
End Transaction

Fig.2 Architecture Diagram for Fraud Detection using Finger Print Recognition

3. PROPOSED SYSTEM

The proposed system is to develop a website which has capability to secure and block the transaction performing by fraudulent user. In proposed model based on secret code and OTP will help to verify fraudulent of transaction during transaction will be going to happen. It comprises with many steps, first is to login into a particular site to purchase goods or services, then choose an item and next step is to go to payment mode where credit card information will be required. After filling all these information, now the page will be directed to proposed fraud detection system which will be installed at bank's server or merchant site [1].

All the information about credit card (Like Credit card number, credit card CVV number, credit card Expiry month and year, name on credit card and secret code which is generated by bank service etc.) will be checked with credit card database. If User entered database is correct then it will ask Secret Code and OTP (One Time Password).

If user entered information will be matched with database information, then transaction will be done securely. And else user transaction will be terminated and transferred to online shopping website. The flowchart of proposed module is shown in Fig. 3

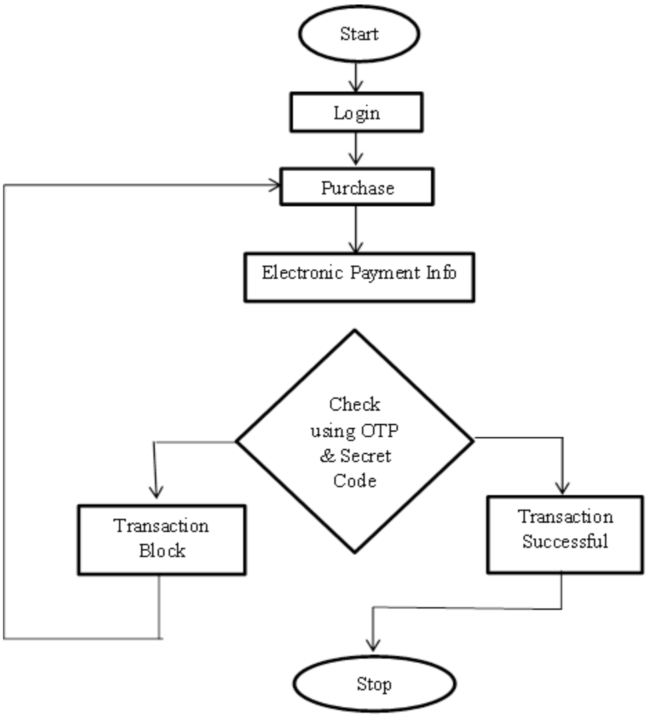

Fig. 3 Flow Chart for Reduce Fraud in Electronic Payment Gateway

4. CONCLUSIONS

As usage of credit cards or online payment become more and more common in every field of the daily life, credit card fraud has become much more rampant. So we need security for any transaction from fraudulent user. In these proposed system we analyzed and detect the fraud in online credit-card transactions in real time. Also generate Secret Code and OTP for transaction.

REFERENCES

[1] Vishal Jain, Gagandeep Singh Narula & Mayank Singh, "Implementation of Data Mining in Online Shopping System Using TANAGRA Tool", *International Journal of Computer Science and Engineering(IJCSE),* Vol 2, Issue 1, 47-58, Feb 2013.

[2] Shaffy Goyal, Namisha Modi, "A Review on Various Classification Algorithms for Online Shopping Data", *International Journal of Computer Application,* Vol 6, March-April 2016

[3] Bharati M. Ramageri, Dr.B. L. Desai, "Role of Data Mining in Retail Sector",*International Journal on Computer Science and Engineering,* Vol. 5, Jan 2013

[4] V. Dheepa, R. Dhanapal, "Behavior Based Credit Card Fraud Detection using Support Vector Machines", *ICTACT Journal on Soft Computing,* Vol 2, July 2012

[5] Mr. P. Matheswaran, Mrs. E. Siva Sankari, Mr. P. Rajesh, "Fraud Detection in Credit Card Using Data Mining Techniques", *International Journal for Research in Science Engineering and Technology,* Vol 2, 11-18, Feb 2015

[6] Priya Ravindra Shimpi, Prof. Vijayalaxmi Kadroli, "Survey on Credit Card Fraud Detection Techniques", *International Journal of Engineering and Computer Science",* Vol-4, Nov 2015, Page No. 15010-15015.

[7] Deepak Pawar, Swapnil Rabse, Sameer Paradkar, Naina Kaushik, "Detection of Fraud In Online Credit Card Transactions", *International Journal of Technical Research And Application,* Vol 4, Issue, March-April-2016, PP 321-323

[8] V. Bhusari, S. Patil, "Study of Hidden Markov Model in Credit Card Fraudulent Detection", *International Journal of Computer Application,* Vol-2, April 2011

[9] Ashlesha Bhingarde, Avnish Bangar, Krutika Gupta, Snigdha Karambe, "Credit Card Fraud Detection using Hidden Markov Model", *International Journal*

of Advanced Research in Computer and Communication Engineering, Vol 4, March 2015

[10] Twinkle Patel, Ms. Ompriya Kale, "A Secured Approach to Credit Card Fraud Detection using Hidden Markov Model", *International Journal of Advanced Research In Computer Engineering & Technology (IJARCET)* , Vol 3, May 2014

[11] 1V.Priyadharshini, G.Adiline Macriga, "An Efficient Data Mining for Credit Card Fraud Detection using Finger Print Recognition ", *International Journal of Advanced Computer Research,* Vol-2, December-2012