A Review on Prevention of Fraud in Electronic Payment Gateway Using Secret Code

Shilpa D. Dhobe[1], Khemutai K. Tighare[2], Sujata S. Dake[3]

[1]*Student, Department of Computer Science and Engineering, Wainganga College of Engineering and Management, Nagpur, India*

[2,3]*Assistant Professor, Department of Computer Science and Engineering, Wainganga College of Engineering and Management, Nagpur, India*

Abstract*: Now a days, the volume of electronic transactions has raised significantly, mainly due to the popularization of electronic commerce (e-commerce), such as online retailers (e.g., Amazon.com, eBay, AliExpress.com). The use of credit cards has increased and it becomes the popular mode of payment for both online and offline purchases. Fraud is one of the major ethical issues in electronic payment Gateway. Fraud essentially involves using deception to dishonestly make a personal gain for oneself and/or create a loss for another. We also observe a significant increase in the number of fraud cases, resulting in billions of dollars' losses each year worldwide. Therefore, it is important and necessary to prevent and use techniques that can assist in fraud detection and prevention. Preventing fraud in real-time is not easy so it is not surprising that many fraud systems have serious limitations. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. In this system credit card numbers for online transactions, other personal and financial information all need to be encrypted. System reduces fraud by using Secret Code. This secret code stored in encryption format so unauthorized user cannot use this secret code. The goal of this paper is to provide a comprehensive review of preventing fraud in Electronic Payment Gateway.

***Keywords*: E-commerce, Electronic payment gateway, Credit card, Secret code.**

1. Introduction

E-commerce is evolving rapidly and now it is reality. Efficient and effective electronic payment services are already established and accepted by businesses and consumers. Advances in e-commerce, expansion of modern technologies and global communication provide a large number of business opportunities, as well as new threats for the banking and financial services. The advancement in the electronic commerce technology, the use of credit cards has increased and it becomes the popular mode of payment for both online and offline purchases. E-commerce provides the capability of buying and selling products, services and information on the Internet by using electronic payment systems. In electronic payment systems the exchange of value is represented by the exchange of data. Credit card transactions have become a standard for Internet and Web based payments. There is millions of credit card transactions processed each day. System architecture of contemporary electronic payment systems is shown in Figure.

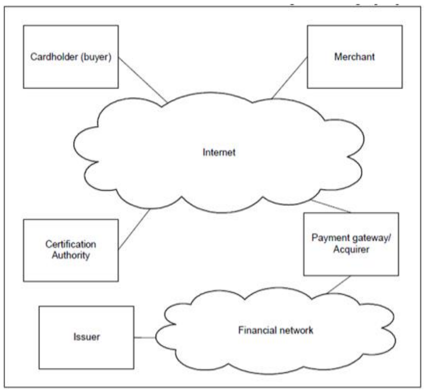

Fig. 1. System architecture of electronic payment systems

Credit card is a plastic-card issued by a bank or nonbanking financial company (NBFC) ready to lend money (give credit) to its customer. It is a suitable alternative for cash payment. It is used to execute transactions which are compiled through electronic devices like a card swapping machine, computer with internet facility, etc.

A. Credit Card Operation

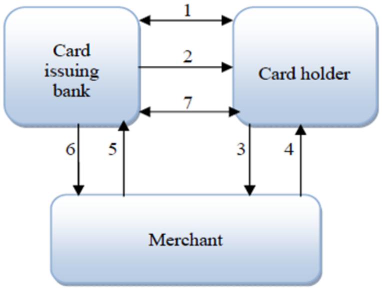

Fig. 2. Credit card operation

1. Contract for credit card

2. Issue of Credit card
3. Purchasing goods
4. Deliver goods
5. Raising of bill
6. Payment for bills
7. Payment of Credit card

The credit card operation consists of the steps as follows:

1. *Contract for credit card:* there is a contract between cardholder and the cared issuing bank regarding limit etc.
2. *Card issue:* Once the contract is finished, the bank issues the credit card to their customer.
3. *Purchasing goods:* A Cardholder purchases goods/services and offers the credit card.
4. *Deliver goods:* A merchant establishment delivers goods once taking a valid credit card and noting the number and taking signatures.
5. *Raising of bill:* The merchant establishment raises the bill for the purchase and sends it to the credit card issuing bank for payment.
6. *Payment for bill:* The issuing bank pays the amount to the merchant establishment.
7. *Payment of Credit card:* The issuing bank raises bill on the credit cardholder and sends it for payment. The credit card holders then pay the amount to the issuing Bank.

Credit card fraud is defined as a transaction when an individual uses another individual. Credit card or corresponding data for payment of goods or services while the owner of the card and the card issuers are not aware of that. There are many types of fraud in electronic payment systems. Fraud can occur in a number of ways including:

- Counterfeit fraud,
- Merchant fraud,
- Card-not-present fraud,
- ATM fraud,
- Internet fraud,
- Lost or stolen cards,
- Identity theft,
- Skimming or copying of electronic data contained on magnetic stripe, and
- MOTO (mail order telephone order) fraud. Fraud prevention describes measures to stop fraud occurring in the first place. When prevention fails then fraud detection comes into play.

Bhatla et al [1] said that the rate at which Internet credit card fraud occurs is 12 to 15 times higher than face-to-face transactions. The 12th annual online fraud report by CyberSource [2] shows that, for most of the current decade, merchant online fraud losses continued to increase, reaching a peak of $4 billion in 2008. According to Siddhartha Bhattacharyya et al. [3] with the growth in credit card transactions, as a share of the payment system, there has also been an increase in credit card fraud.

Fraud is often mistakenly considered a victimless crime. However, fraud can have considerable social and psychological effects on individuals, businesses and society. For example, when a fraud causes the collapse of a major company, numerous individuals and businesses can be affected.

Fraud deals with cases involving criminal purposes that, mostly, are difficult to identify. Credit cards are one of the most famous targets of fraud but not the only one; fraud can occur with any type of credit products, such as personal loans, home loans, and retail. Furthermore, the face of fraud has changed dramatically during the last few decades as technologies have changed and developed. A critical task to help businesses, and financial institutions including banks is to take steps to prevent fraud. We also testify a huge increase in the number of online frauds, resulting in billions of dollars losses each year worldwide. Therefore, it is important and necessary to developed and apply techniques that can assist in fraud detection, which reduce the frauds and help the people by making safe online transaction.

B. *Types of Fraud*

1) *Application Fraud*

This kind of fraud happens once someone falsifies an application to acquire a credit card. Application fraud is committed in 3 ways:

Assumed identity, wherever an individual illicitly obtains personal info of another person and opens accounts in his or her name, using partly legitimate info.

Financial fraud, wherever an individual provides false info regarding his or her financial standing to acquire credit. Not-received items (NRIs) additionally known as postal intercepts occur once a card is purloined from the postal service before it reaches its owner's destination.

2) *Lost/ Stolen Cards*

A card is lost/stolen once a legitimate account holder receives a card and loses it or somebody steals the card for criminal functions. This sort of fraud is in essence the best way for a fraudster to get hold of alternative individual's credit cards without investment in technology. It is also maybe the toughest kind of ancient credit card fraud to tackle.

3) *Account Takeover*

This type of fraud happens once a fraudster illicitly obtains a valid customers' personal info. The fraudster takes control of (takeover) a legitimate account by either providing the customers a/c.no or the card number. The fraudster then contacts the card issuer, masquerading as the real cardholder, to ask that mail be redirected to a new address. The person who commits the fraud reports card lost and asks for a replacement to be sent.

4) *Identity theft*

Identity theft/fraud refer to crime in which fraudster illegally obtains and uses another person personal information in some way that involves deception or fraud to gain something of value. Identity theft/fraud is the most serious crime for the person whose information is stolen as well as the financial institution.

5) *Phishing*

Phishing is a well known technique for obtaining confidential information from a user by posing as a trusted authoring. Phishing is an attempt by fraudster to „fish" for your baking details through emails with attachment or hyperlinks. The e-mail appears to be send from legitimate organization to trick people in order to reveal sensitive information. On clicking the attachment or the hyperlink the computer system gets infected with malware. During the next online transaction, the malware will activate and steal private and personal financial information, including credit card numbers, PIN number which is used by fraudster to steal money from the account. Malware or "Malicious Software" is software which includes computer viruses, worms, Trojan Horses, spyware and other malicious software.

6) Spoofing or Website cloning

This is an act of creating a hoax web site or to say duplication of a website for criminal use. The fraudsters use legitimate companies name, logos, graphics and even code. This usually take form of know chat room or trade sites where in people would innocently giving out personal information to criminals or make a fake purchase of a product the does not exist. Site cloning is the process where fraudsters close whole site or simply the pages from which the customer made a purchase. There is no option left with the customers to believe that they are not dealing with the company that they wished to purchase goods or services from because the pages that they are viewing are somehow.

7) Skimming

Another kind of fraud being committed is skimming which is fast emerging as the most popular form of credit card fraud. Mostly, fraud cases of Counterfeit fraud involve skimming. It is a method where the actual data on a card's magnetic stripe is electronically copied onto another. Fraudster(s) does this even as the customer is waiting for the transaction to be validated through the card terminal. Card holder doesn't t know about this activity and it is very difficult for customer(s) to identify. In some of the cases, details obtained by skimming are used to carry out fraudulent card not-present (CNP) transactions by fraudsters.

2. Literature review

A. Online Fraud

Credit is a method of selling goods or services without the buyer having cash in hand. A credit card is only an automatic way of offering credit to a

Consumer. Today, every credit card carries an identifying number that speeds shopping transactions. According to Encyclopedia Britannica (no date), "the use of credit cards originated in the United States during the 1920s, when individual firms, such as oil companies and hotel chains, began issuing them to customers."

Credit card fraud is divided into two types: offline fraud and online fraud. Offline fraud is committed by using a stolen physical card at storefront or call center. In most cases, the institution issuing the card can lock it before it is used in a fraudulent manner. Online fraud is committed via web, phone shopping or cardholder not- present. Only the card's details are needed, and a manual signature and card imprint are not required at the time of purchase. In the credit card business, fraud occurs when a lender is fooled by a borrower offering him/her purchases, believing that the borrower credit card account will provide payment for this purchase. Ideally, no payment will be made. If the payment is made, the credit card issuer will reclaim the amount paid.

B. Payment Gateway

A payment gateway, also known as the processor or credit card processor, connects the merchant's website and shopping cart, the acquiring bank (merchant's bank), and the issuing bank (cardholder's bank). The payment gateway handles all communication messages between these entities. By handling the two key parts of credit card processing, authorization and payment settlement, the payment gateway is the key link in an online transaction.

During authorization, credit card information from the merchant's website is sent to the payment gateway by the shopping cart, which verifies the card information and then sends a request to the cardholder's bank for the card to be charged. If the card information is valid and the customer's credit is sufficient, then the credit card company sends an approval to the payment gateway, which in turn communicates with the shopping cart and confirms the authorization for the purchase. The payment gateway then initiates a payment settlement (funds transfer) to allow the transfer of funds from the customer's credit card account to the merchant's bank account.

3. Related work

Problem of detecting fraudulent transactions occurs after they have been focused to fraud prevention methods and relevant processes. There is immense literature on wide range of security methods to look after transactions from unauthorized use or exposure of their private/secure information and consequent valuable resources. With the increase in e-commerce sales the merchants face challenges to reduce frauds in e-payment transactions. E-frauds start with diversion of personal information. A poorly protected computer, a trash or recycling bin, an email message or chat on internet exposes to fraud. It is impossible to totally eliminate the chance of fraud but timely measures taken can reduce the frauds. Fraud prevention involves taking measures to stop fraud from occurring and while fraud prevention fails then the merchant takes steps to detect the frauds quickly and stop it as soon as possible. Fraud prevention and detection involves planning, detecting and avoiding risk.

A. Hidden Morkov Model

Twinkle Patel, Ms. Ompriya Kale [6] 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 [5] 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 [6].

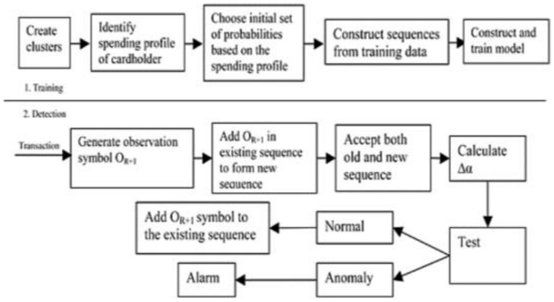
Create clusters
Identify spending profile of cardholder
Choose initial set of probabilities based on the spending profile
Construct sequences from training data
Construct and train model
1. Training
2. Detection
Transaction
Generate observation symbol O_{R+1}
Add O_{R+1} in existing sequence to form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

Fig. 3. Process flow of credit card fraud detection system using HMM

As shown in Fig. 3 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.

B. *Genetic algorithms and other algorithms*

Algorithms are often recommended as predictive methods as a means of detecting fraud. One algorithm that has been suggested by Bentley et al. (2000) is based on genetic programming in order to establish logic rules capable of classifying credit card transactions into suspicious and non-suspicious classes. Basically, this method follows the scoring process. In the experiment described in their study, the database was made of 4,000 transactions with 62 fields. As for the similarity tree, training and testing samples were employed. Different types of rules were tested with the different fields. The best rule is the one with the highest predictability. Their method has proven results for real home insurance data and could be one efficient method against credit card fraud. Chan et al. (1999) also developed an algorithm to predict suspect behavior. The originality of their research is that the model is evaluated and rated by a cost model, whereas other studies use evaluation based on their prediction rate/the true positive rate and the error rate/the false negative rate. Wheeler & Aitken (2000) developed the idea of combining algorithms to maximize the power of prediction. In their article, they present different algorithms: diagnostic algorithms, diagnostic resolution strategies, probabilistic curve algorithms, best match algorithms, negative selection algorithms, and density selection algorithms. They conclude from their investigation that neighborhood-based and probabilistic algorithms have been shown to be appropriate techniques for classification, and may be further enhanced using additional diagnostic algorithms for decision-making in borderlines cases, and for calculating confidence and relative risk measures.

C. *Clustering techniques*

Bolton & Hand (2002) suggest two clustering techniques for behavioral fraud. The peer group analysis is a system that allows identifying accounts that are behaving differently from others at one moment in time whereas they were behaving the same previously. Those accounts are then flagged as suspicious. Fraud analysts have then to investigate those cases. The hypothesis of the peer group analysis is that if accounts behave the same for a certain period of time and then one account is behaving significantly differently, this account has to be notified. Breakpoint

Analysis uses a different approach. The hypothesis is that if a change of card usage is notified on an individual basis, the account has to be investigated. In other words, based on the transactions of a single card, the break-point analysis can identify suspicious behavior. Signals of suspicious behavior are a sudden transaction for a high amount, and a high frequency of usage.

D. *Outlier Detection*

An outlier is an observation that deviates so much from other observations as to arouse suspicion that it was generated by a different mechanism. Unsupervised learning approach is employed to this model. Usually, the result of unsupervised learning is a new explanation or representation of the observation data, which will then lead to improved future responses or decisions. Unsupervised methods do not need the prior knowledge of fraudulent and non-fraudulent transactions in historical database, but instead detect changes in behavior or unusual transactions.

These methods model a baseline distribution that represents normal behavior and then detect observations that show greatest departure from this norm. Outliers are a basic form of non-standard observation that can be used for fraud detection. In supervised methods, models are trained to discriminate between fraudulent and non-fraudulent behavior so that new observations can be assigned to classes. Supervised methods require accurate identification of fraudulent transactions in historical databases and can only be used to detect frauds of a type that have previously occurred. An advantage of using unsupervised methods over supervised methods is that previously undiscovered types of fraud may be detected. Supervised methods are only trained to discriminate between legitimate transactions and previously. Known fraud. Bolton and Hand proposed unsupervised credit card fraud detection, using behavioral outlier detection techniques. Abnormal spending behavior and frequency of transactions will be identified as outliers, which are possible fraud cases.

E. Fraud detection using finger print recognition

Priyadharshini, and G. Adiline Macriga [6] 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.

4. Proposed system

In proposed system, whenever a new user use credit card and debit card for online transaction then all details are cross checked. This proposed model based on secret code that will help to verify fraudulent of transaction when transaction takes place. In This system it develops a website which provides security and blocks the transaction performing by fraudulent user. The first step 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 credit card information like Credit card number, name on credit card, credit card Expiry month and year, credit card CVV number and secret code which is generated by bank service etc. will be checked with credit card database. Now data entered by User is correct then it will ask Secret Code to user. If user entered information that is credit card information and secret code 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.

5. Conclusion

In recent times credit cards becomes the most popular means of payment and if credit card transactions increase, so too do frauds. Credit card fraud has become more and more widespread in recent years. In this paper the problem of fraud in electronic payment systems is addressed. Reducing fraud is a very important goal in electronic payment systems, which may be achieved by using prevention and detection techniques. Therefore, fraud prevention and detection techniques have to be proactive and always be ready to minimize fraudulent activities. Combination of different techniques gives best results. In this proposed system we check, analyzed and detect the fraud in online credit-card transactions. Also generate Secret Code to secure and block the transaction performing by fraudulent user.

References

[1] Linda Delamaire (UK), Hussein Abdou (UK), John Pointon (UK) Banks and Bank Systems, Volume 4, Issue 2, 2009.

[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] 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, March-April-2016, pp. 321-323.

[4] 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.

[5] 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, Vol 3, May 2014

[6] Evandro Caldeira Federal Center of Technological Education of Minas Gerais (CEFET-MG) Computing Department Belo Horizonte, MG, Brazil.

[7] Gabriel Brand˜ao Federal Center of Technological Education of Minas Gerais (CEFET-MG) Computing Department Belo Horizonte, MG, Brazil Adriano C. M. Pereira Federal University of Minas Gerais (UFMG) Dept. of Computer Science Belo Horizonte, MG, Brazil.

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

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

[10] Priya Ravindra Shimpi, Prof. Vijayalaxmi Kadroli, "Survey on Credit Card Fraud Detection Techniques", International Journal of Engineering and Computer Science", Vol. 4, Nov. 2015, pp. 15010-15015.