ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
*Vol. 1, Issue 5, July 2013*

# Method and System for Detecting Fraud in Credit Card Transaction

Vivek Kumar Prasad

Assistant Professor, Dept. Of CE, Institute of Technology, Nirma University, Ahmedabad, India

**ABSTRACT**: Due to a rapid advancement in the electronic commerce technology. Credit card becomes the most popular mode of payment for both online as well as regular purchase. Cases of fraud associated with it are also rising. In this paper I am introducing the concept of three level of security, the first level is the static User name or password, and in the second level it uses Hidden Markov Model (HMM) and shows how it can be used for the detection of frauds. An HMM is initially trained with the normal behaviour of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. And to reduce the false positive transactions we will send the dynamic password, which can be send through the use of web services to the user's mobile phone number instantly and he/she has to enter same password for getting the authorization from the bank side and suppose if due to the heavy load on the server side , if the user does not get the password in its mobile phone within the given stipulated time , then after a little time interval some personnel questions(either security question or images) will be asked which can be answered by the end user

Keywords*:* Hidden Markov Model (HMM), Static username /password, false positive, security question, security picture, dynamic password.

## I. INTRODUCTION

While performing online transaction using a credit card issued by bank, the transaction may be either Online Purchase or transfer .The online purchase can be done using the credit or debit card issued by the bank or the card based purchase can be categorized into two types Physical Card and Virtual Card. In both the cases if the card or card details are stolen the fraudster can easily carry out fraud transactions which will result in substantial loss to card holder or bank. In the case of Online Fund Transfer a user makes use of details such as Login Id, Password and transaction password. Again here if the details of the account be miss used then, as a result, it which will give rise to fraud transaction.

Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft.

The fraud begins with either the theft of the physical card or the compromise of data associated with the account, including the card account number or other information that would routinely and necessarily be available to a merchant during a legitimate transaction. The compromise can occur by many common routes and can usually be conducted without tipping off the card holder, the merchant or the issuer, at least until the account is ultimately used for fraud. A simple example is that of a store clerk copying sales receipts for later use. The rapid growth of credit card use on the Internet has made database security lapses particularly costly; in some cases, millions of accounts have been compromised.

Stolen cards can be reported quickly by cardholders, but a compromised account can be hoarded by a thief for weeks or months before any fraudulent use, making it difficult to identify the source of the compromise. The cardholder may not discover fraudulent use until receiving a billing statement, which may be delivered infrequently.

## II.BASICS AND DEFINITIONS

In the three level of security the first level is Static username /password (it can be the Personal Identification Number also), these are the credentials which are used to authenticate and authorize the customers. For example the username and password are the credentials which are used to authenticate the user's rights to accessing the account. Authorization means after checking the credentials, if the account details are correct then allowing them to access their recourses.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
*Vol. 1, Issue 5, July 2013*

The second level is all about Hidden Markov Model, which is a double embedded stochastic process with two hierarchy levels. It can be used to model much more complicated stochastic processes as compared to a traditional Markov Model [4]. An HMM has a finite set of states governed by a set of transition probabilities .In a particular state ,an outcome or observation can be generated according to an associated probability distribution. It is only the outcome and not the state that is visible to an external observer. Each state has a probability distribution over the possible output tokens. Therefore the sequence of tokens generated by a HMM gives some information about the sequence of states. Note that the adjective 'hidden' refers to the state sequence through which the model passes, not to the parameters of the model, even if the model parameters are known exactly, the model is still 'hidden'.HMM based applications are common in various areas such as speech recognition, bioinformatics and genomics [3].

*A. HMM and Fraud Detection*

In fraud detection system HMM is initially trained with the normal behaviour of a cardholder [1]. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. Then the third level will be evoked which is Dynamic password, it is a random generated number or password, which is send to the user or customer's (or who so ever may be the owner of the credit Card.) mobile phone through the help of the web services, just to ensure that the correct user is using the card at that instant of time. Apart from this the other concept are security pictures and security questions which will come into the picture when the dynamic password will not reach to the user's mobile phone within the given stipulated time.

The following are some aspects that can be solved by the above mentioned technique.

*B. Stolen Cards*

When a credit card is lost or stolen, it remains usable until the holder notifies the issuer that the card is lost. Most issuers have free 24-hour telephone numbers to encourage prompt reporting. Still, it is possible for a thief to make unauthorized purchases on a card until it is cancelled. Without other security measures, a thief could potentially purchase thousands of dollars in merchandise or services before the cardholder or the card issuer realize that the card is in the wrong hands [6].

*C. Compromised Accounts*

Card account information is stored in a number of formats. Account numbers are often embossed or imprinted on the card, and a magnetic stripe on the back contains the data in machine readable format. Fields can vary, but the most common include.1) Name of the card holder 2) Account number 3) Expiration date.

*D. Card not Present*

The mail and the Internet are major routes for fraud against merchants who sell and ship products, and impacts legitimate mail-order and Internet merchants. If the card is not physically present (called CNP, Card Not Present) the merchant must rely on the holder (or someone purporting to be so) presenting the information indirectly, whether by mail, telephone or over the Internet. While there are safeguards to this, it is still more risky than presenting in person, and indeed card issuers tend to charge a greater transaction rate for CNP [6], because of the greater risk. To many people's surprise, telephone ordering is the most risky, far more risky than the Internet.

*E. Identity Theft*

Identity theft [6] can be divided into two broad categories: Application fraud and account takeover.

Application Fraud: Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Or they may create counterfeit documents.

Account Takeover: Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, then contacting their card issuer masquerading as the genuine cardholder, and asking for mail to be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent.

*F. Skimming*

Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant. The thief can procure a victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' credit card numbers. Common scenarios for skimming are restaurants or shopping malls where the skimmer has possession of the victim's credit card out of their immediate view.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
*Vol. 1, Issue 5, July 2013*

The thief may also use a small keypad to unobtrusively transcribe the 3 or 4 digits Card Security Code which is not present on the magnetic strip [6].

*G. Carding*

Carding [6] is a term used for a process to verify the validity of stolen card data. The thief presents the card information on a website that has real-time transaction processing. If the card is processed successfully, the thief knows that the card is still good. The specific item purchased is immaterial, and the thief does not need to purchase an actual product, a Web site subscription or charitable donation would be sufficient. The purchase is usually for a small monetary amount, both to avoid using the card's credit limit, and also to avoid attracting the card issuer's attention.

*H. BIN Attack*

Credit cards are produced in BIN ranges [2]. Where an issuer does not use random generation of the card number, it is possible for an attacker to obtain one good card number and generate valid card numbers by changing the last four numbers using a generator. The expiry date of these cards would most likely be the same as the good

## III.MPLEMENTATION

***How HMM works?***

HMM keeps track of the spending pattern on every card and it figures out any inconsistency with respect to the "usual" spending patterns. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability [5]. Then it will issue an alarm which indicates that something wrong has happened with the credit card usages, but in this paper instead of alarm, we can send the dynamic password to the users mobile phone, so that we can reduce the number of false positive, false positive means an alarm or alert that indicates that an attack is in progress or that an attack has successfully occurred when in fact there was no such attack. In Hidden Markov Model (HMM), 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 an HMM).Figure 3.1 indicates the process flow diagram for training the HMM.

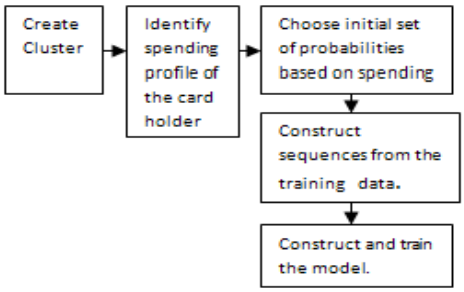



Figure 3.1 Process flow diagram for training HMM.

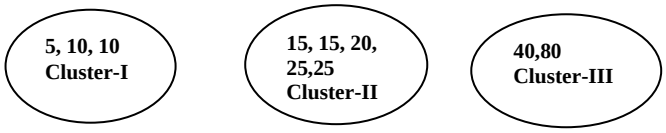
We categories the profiles of the users as low spending profile, medium spending profile, high spending profile and the intruder itself. The spending profile of the individual card holder is used to obtain an initial estimate of their profiles.

| Transaction number. | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Dollar Amount. | 40 | 25 | 15 | 5 | 10 | 25 | 15 | 20 | 10 | 80 |

TABLE:3.1 TRANSACTION TABLE

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
*Vol. 1, Issue 5, July 2013*




CLUSTER I: LOW SPENDING PROFILE
CLUSTER II: MEDIUM SPENDING PROFILE
CLUSTER III: HIGH SPENDING PROFILE

Figure: 3.2 CLUSTERING

*Clustering*

For example, let us take O1, O2, O3,O4…..Or be the sequences of transactions done by the card holder, of length r, and let O[r+1] be the symbol generated by the new latest transaction. To form another sequence of length r we drop O1 and append O[r+1] in the sequence and generate a new sequence from as O2, O3,O4……O[r+1]. And then calculate the differences in between both the old and new sequences to identify whether the transaction is genuine or not. As shown above in the figure 3.2. We have taken the r value as 10.As shown in Table 3.1, which indicates the transactions done by the user and for these transactions, we are creating three clusters. Where the cluster I is the low spending profile cluster, cluster II is the medium spending profile cluster and cluster III is the high spending profile cluster as shown in figure 3.2. So in the above example cluster 2 have the maximum percentage of the transactions. So we can conclude that the user comes under the cluster 2 or he/she is in medium spending profile. So if the new transaction comes, then again clusters are formed and differences are noted down. If there is no difference then the transaction will be committed and if the difference are found (i.e. the profile is found to change) then the dynamic password has to be send to the users mobile phone for the sake of identifying the genuine user. As indicated in figure 3.2

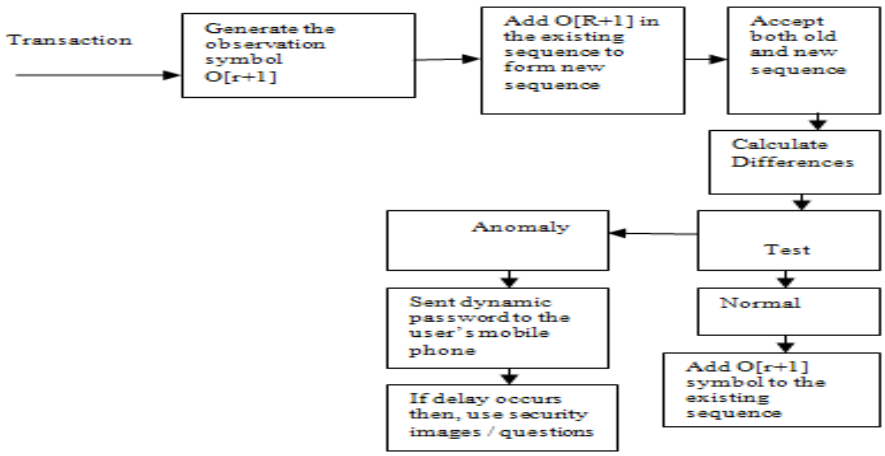



Figure 3.2 Process flow diagram for detection of fraud through HMM

*Dynamic Password*

In case of dynamic 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 just to ensure that the correct user is using the card at that instant of time.He/she has to enter the same password for getting the authorization from the bank side and suppose if due to the heavy load on server side if the user does not get the password in its mobile phone within the given stipulated time, then after a little time interval some personnel questions (security questions/ images) will be asked which can be answered by the users and these security questions/images should match to the questions/images, which are filled/selected by the customer at the time of opening the account.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
*Vol. 1, Issue 5, July 2013*

## IV. CONCLUSION

In this paper I proposed an approach which focuses to online transaction using a credit card issued by bank, the transaction may be either online Purchase or transfer. Where the three level of security has to be implemented, the first one is static password, second one is HMM (Hidden Markov Model) and if the HMM detect any fraud, then the third level will come into the picture where dynamic password has to be used, followed by the security question or the security images, why I am using security images, because in some cases machines from where we were doing transaction will not have the alphabet keypads. So the answer for the security questions will not be typed in such cases. As a result, if the user has the flexibility of selecting any picture through touch screen or by any other means it could work .The limitation of the use of three security level may results to delay in the online purchase or online transferring of the amount. But these delays are negligible because we are focusing more on security. Such a survey will enable us to build secure approach for identifying fraudulent credit card transactions.

## REFERENCES

**[1]** Abhinav Srivastava,Amlan Kundu,Shamik Sural and Arun K Majumdar," Credit Card Fraud Detection Using Hidden Markov Model,"IEEE Transactions On Dependable And Secure Computing ,vol.5 No.1,January-March 2008.

[2] "Credit Card Fraud," http:// en.wikipedia.org/wiki/Credit_card_fraud

[3] L.R Rabiner,"A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognotion," proc.IEEE, vol.77, no.2,pp. 257-286,1989

[ 4] Raj Jain,The Art of Computer Systems Performance Analysis,John Wiley and Sons,Chapter 3,2010.

[5]S.Benson Edwin Raj,A.Annie Portia, "Analysis on Credit Card Fraud Detection Methds", International Conference on ComputerCommunication and Electrical Technology-ICCCET2011,March 2011

[6] "Types of Credit Card Fraud,"http://www.monetos.co.uk/financing /credit-cards/fraud-protection/types.