www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 12 Dec 2015, Page No. 15158-15160

"Banking Expert System"With credit card fraud detection using HMM algorithm

Priya Ravindra Shimpi, Prof. Vijayalaxmi Kadroli

M.E. Information Technology
Terna Engineering College,
navi mumbai Nerul, India
priya.ravindra.shimpi@gmail.com
Information Technology
Terna Engineering College,
navi mumbai Nerul, India
udachanv@gmail.com

Abstract: Due to rapid advancement in electronic commerce technology. Most of the transactions in the banking are done online. As there are many service provider in banking so user must analyze the performance and choose the best among them. Also Credit cards become the most popular mode of payment for both online and regular purchase.

In this paper we are 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 behavior 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.

1. 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.

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.

2. Implementation

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.

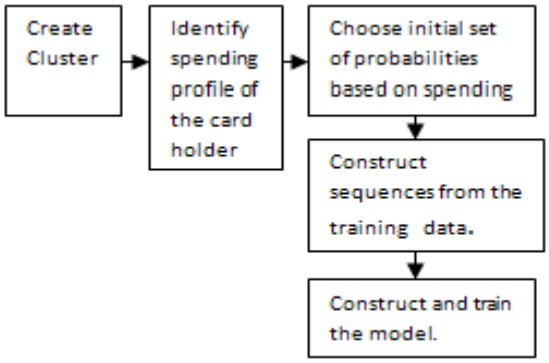
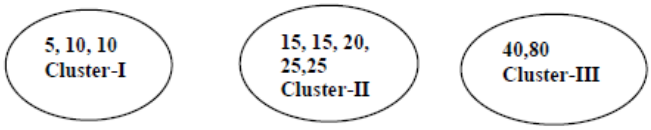


Figure 3.1 Process flow diagram for training HMM.

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 No.	1	2	3	4	5	6	7	8	9	10
Amount in thousand	20	25	15	5	10	25	15	20	10	80

TABLE:3.1 TRANSACTION TABLE



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 cluster2 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

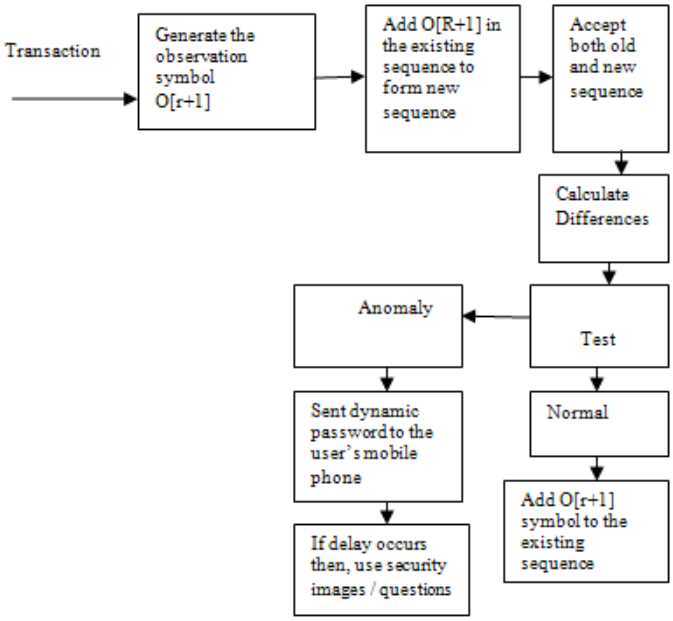


Figure 3.2 Process flow diagram for detection of fraud through HMM

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.

CONCLUSION

In this paper we 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

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.