'FUTURIZM-2014, (14TH & 15TH March 2014), 'P.D.E.As College of Engineering, Manjari[Bk]', 'IIP Cell,'Manjari Road, Hadapsar, Pune-412307. India.','Chief Editor:Dr.K.R.Harne', Editors: Prof R V Patil, Prof Niraja Jain

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-11 , August, 2014

Credit Card Fraud Detection Using Hidden Markov Model (HMM)

Komal Mule[1], Madhuri Kulkarni[2]
[1]Computer Department, Dr. D.Y.Patil School Of Engineering & Technology, PG Student, Pune, India
(physicskomal7@gmail.com)
[2]Alard College Of Engineering & Management, PG Student, Pune, India
(Madhuri.kulkarni85@gmail.com)

Abstract - **Today, the improvements in technology have brought up a revolution around the globe. Almost all activities are now going online with the help of technology. Online shopping, file transfer etc. all these factors have greatly in influenced the businesses situated worldwide. Almost every person today possess a credit card and widely uses the same for making online purchases, as it has become the most popular mode of payment in almost all online applications. But however there are also some risks and threats associated with credit cards, mainly the chances of committing frauds have greatly increased. In real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. Implementation of efficient fraud detection systems has thus become crucial for all credit card issuing banks to minimize their losses. Many modern techniques based on Artificial Intelligence, Data mining, Fuzzy logic, Machine learning, Sequence Alignment, Genetic Programming etc., has evolved in detecting various credit card fraudulent transactions. This paper presents technique used in credit card fraud detection mechanism using hidden markov model.**

Keywords - **Online Shopping, Credit Card, Hidden Markov Model, Fraud detection, anomaly intrusion detection systems (AIDSs)**

I. INTRODUCTION

Credit-card-based purchases can be categorized into two types:

- Physical card
- Virtual card.

In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment [7]. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the credit card. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss. 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. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. 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.

II. LITERATURE SURVEY

Gosh and Reilly have proposed credit card fraud detection with a neural network [6]. In case of the existing system the fraud is detected after the fraud is done i.e., the fraud is detected after the complaint of the card holder. And so the card holder faces a lot of trouble before the investigation finish. And also as all the transaction is maintained in a log, we need to maintain a huge data. The problem with the above mentioned approach is that they require labeled data for both genuine, as well as fraudulent transactions, to train the classifiers. Getting real-world fraud data is one of the biggest problems associated with credit card fraud detection [1].

Also, these approaches cannot detect new kinds of frauds for which labeled data is not available. In contrast, we present a Hidden Markov Model (HMM)-based credit card Detection model i.e. CCFD, which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending behavior. We model

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-6 , March, 2014

a credit card transaction processing sequence by the stochastic process of an HMM. The details of items purchased in individual transactions are usually not known to an FDS running at the bank that issues credit cards to the cardholders. [2]

Aleskerov et al. brought CARDWATCH, a database mining system used for credit card fraud detection. The system provides an interface to a variety of commercial databases and is based on a neural learning module. Kim and Kim have recognized skewed distribution of data and blend of legitimate and fraudulent transactions as the two main reasons for the complication of credit card fraud detection [10]. Based on this observation, they use fraud density of real transaction data as a confidence value and generate the weighted fraud score to reduce the number of misdetections [3]. Anomaly intrusion detection systems (AIDSs) have the potential to discover novel attacks, AIDSs suffer from the lack of generalization capability and the presence of high false alarm rates [8].

A. HMM

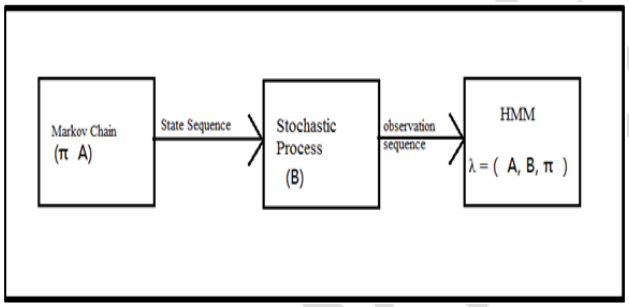

Fig 1: A Hidden Markov Model

As described in figure 1. A Hidden Markov Model is a finite set of states each state is linked with a probability distribution. Transitions among these states are governed by a set of probabilities called transition probabilities. In a particular state a possible outcome or observation can be generated which is associated symbol of observation of probability distribution. It is only the outcome, not the state that is visible to an external observer and therefore states are "hidden" to the outside; hence the name Hidden Markov Model. Hence, 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.

- Low (l),
- Medium (m) ,
- 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.

III. SYSTEM ARCHITECTURE

A. Proposed System

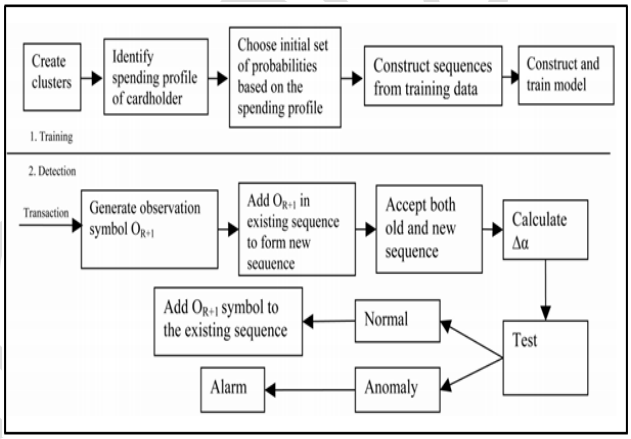

Fig 2: Proposed System

An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the FDS. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc. If the FDS confirms the transaction to be malicious, it raises an alarm, and the issuing bank declines the transaction. The concerned cardholder may then be contacted and alerted about the possibility that the card is compromised. In this section, we explain how HMM can be used for credit card fraud detection [2-5].

After the HMM parameters are learned, we take the symbols from a cardholder's training data and form an initial sequence of symbols. Let o1, o2----or be one such sequence of length R. This recorded sequence is formed from the cardholder's transactions up to time t. We input

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-6 , March, 2014

this sequence to the HMM and compute the probability of acceptance by the HMM. Let the probability be 1, which can be written as follows:

$$\alpha 1 = P(o1, o2, \text{----or})$$

Let or+1 be the symbol generated by a new transaction at time t+1. To form another sequence of length R, we drop O1 and append or+1 in that sequence, generating o2, o3----, or+1as the new sequence. We input this new sequence to the HMM and calculate the probability of acceptance by the HMM. Let the new probability,

$$\alpha 2 = P(o2, o3, \text{----or+1})$$

Let $\Delta \alpha = \alpha 1 - \alpha 2$ .If $\Delta \alpha > 0$, it means that the new sequence is accepted by the HMM with low probability, and it could be a fraud. [2] The newly added transaction is determined to be fraudulent, otherwise the transaction is genuine. The architecture of the system looks like as shown in Figure 2.

B. Flow Of System

The flow of proposed system is as shown in figure 3. The proposed model consists of two modules.

- Online Shopping
- Fraud Detection System

In Online Shopping module login takes place at the online shopping site. After adding items to the cart user proceeds towards payment of goods. Here user fills the information about credit card. After this information is filled, the page gets directed towards the fraud detection system.

When the page gets directed towards the fraud detection system, the information like CVV number, credit card number, credit card expiry month and year, etc. has to be filled. If the user has entered the credit card information correctly then the user will be asked for a PIN (personal Identity Number). Then PIN will be verified. The HMM will start working after 10 transaction. If module finds any transaction fraudulent then user is asked to answer particular question. If answers are given correctly then it genuine transaction else it is fraudulent [4].

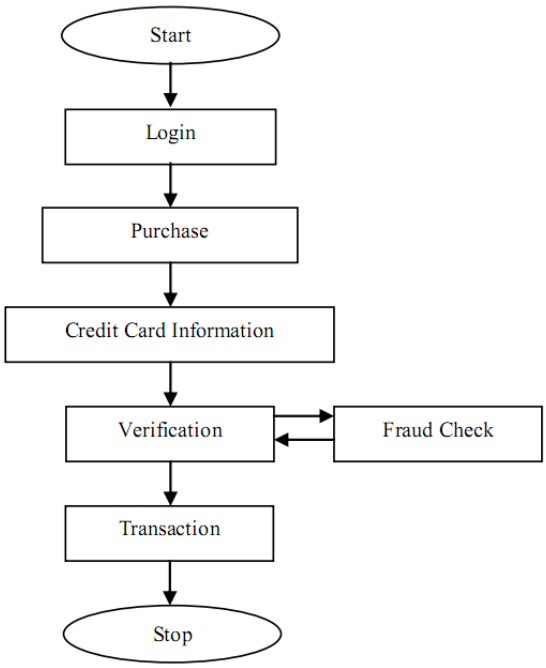

Fig 3: Flow of System

IV. METHODOLOGY

As business processing of credit card fraud detection system runs on a credit card issuing bank site or merchant site. Each arriving transaction is submitted to the fraud detection system for verification purpose. The fraud detection system accept the card details such as credit card number, cvv number, card type, expiry date and the amount of items purchase to validate, whether the transaction is genuine or not. The implementation techniques of Hidden Markov Model in order to detect fraud transaction through credit cards, it create clusters of training set and identify the spending profile of cardholder. The number of items purchased, types of items that are bought in a particular transaction are not known to the Fraud Detection system, but it only concentrates on the amount of item purchased and use for further processing. It stores data of different amount of transactions in form of clusters depending on transaction amount which will be either in low, medium or high value ranges. It tries to find out any variance in the transaction based on the spending behavioral profile of the cardholder. The probabilities of initial set have chosen based on the spending behavioral profile of card holder

International Journal of Innovative Technology & Adaptive Management (IJITAM)
ISSN: 2347-3622, Volume-1, Issue-6 , March, 2014

and construct a sequence for further processing. If the fraud detection system makes sure that the transaction to be of fraudulent, it raises an alarm, and the issuing bank declines the transaction. For the security purpose, the Security information module will get the information features and its store's in database. The flow of the system looks like as shown in Figure 3. It is suitable for anomaly detection with high detect rate and low false alarm rate [9].

V. ADVANTAGES

- The detection of the fraud use of the card is found much faster that the existing system.
- In case of the existing system even the original card holder is also checked for fraud detection. But in this system no need to check the original user as we maintain a log.
- The log which is maintained will also be a proof for the bank for the transaction made.
- We can find the most accurate detection using this technique.
- This reduces the tedious work of an employee in the bank.

VI. RESULTS

By using hidden markov model for credit card fraud detection we get very low false alarms. If any anomaly is observed in transaction then user of credit card gets sms and mail that contains one time password (OTP). If genuine user is doing the transaction then he can enter OTP while doing the purchase transaction. If genuine user is not doing the transaction then fraud is quickly detected.

VII. DISCUSSION & CONCLUSION

In this paper brief discussion of Hidden Markov Model is given which reflects the advantage and simplicity of HMM. The study shows that HMM works on human behavior while doing online shopping which will be a base for further enhancement of the technique, and resulting into a better detection method. The future work on this can to be to make HMM more secure and covering other aspects of human behavior.

REFERENCES

[1] *S.Benson Edwin Raj, A. Annie Portia, "Analysis on Credit Card Fraud Detection Methods", IEEE International Conference on Computer, Communication and Electrical Technology, IEEE March 2011.*

[2] *Credit Card Fraud Detection Using HMMAuthors: Abhinav Srivastava, Amlan Kundu, Shamik Sural. IEEE Transaction on Dependable & Secure Computing.Volume: 5 Publication Year: 2008*

[3] *Anshul Singh, Devesh Narayan, "A Survey on Hidden Markov Model for Credit Card Fraud Detection" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-3, February 2012*

[4] *V. Bhusari, S. Patil, "Study of Hidden Markov Model in Credit Card Fraudulent Detection" International Journal of Computer Applications (0975 – 8887) Volume 20– No.5, April 2011*

[5] *B.Sanjaya Gandhi, R.Lalu Naik, S.Gopi Krishna, K.lakshminadh "Markova Scheme for Credit Card Fraud Detection" UACEE International Journal of Computer Science and its Applications.*

[6] *S. Gosh and D.L. Reilly, "Credit Card Fraud Detection with a Neural-Network," Proc. 27th Hawaii Int'l Conf. System Sciences: Information Systems: Decision Support and Knowledge-Based Systems.*

[7] *Tej Paul Bhatla, Vikram Prabhu & Amit Dua "Understanding CreditCard Frauds" Cards Business Review#2003–01, June 2003*

[8] *Mohammad Al-Subaie and Mohammad Zulkernine " Efficacy of Hidden Markov Models Over Neural Networks in Anomaly Intrusion Detection"*

[9] *Fanping Zeng, Kaitao Yin, Minghui Chen, Xufa Wang," A New Anomaly Detection Method Based on Rough Set Reduction and HMM" 2009 eight IEEE ACIS International conference on Computer and Information Science.*

[10] *Minority Report in Fraud Detection: Classification of Skewed Data. C. Phua, D. Alahakoon, and V. Lee. 2004.*