



**INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH
TECHNOLOGY**

**CREDIT CARD FRAUD DETECTION USING HIDDEN MARKOV MODEL
AND ENHANCED SECURITY FEATURES**

Ashish Thakur*, Bushra Shaikh, Vinita Jain, A.M.Magar

Sinhgad Academy of Engineering, Kondhwa-Saswad Road, Pune, Maharashtra 411048, India

Sinhgad Academy of Engineering, Kondhwa-Saswad Road, Pune, Maharashtra 411048, India

Sinhgad Academy of Engineering, Kondhwa-Saswad Road, Pune, Maharashtra 411048, India

Sinhgad Academy of Engineering, Kondhwa-Saswad Road, Pune, Maharashtra 411048, India

Abstract

The most accepted payment mode is credit card for both offline and online in today's world, it will provide cashless shopping at every shop across the world. It will be the most suitable way to do online shopping, paying bills, and performing other related tasks. Hence risk of fraud transactions using credit card has also been increasing. In the prevailing credit card fraud detection processing system, fraudulent transaction will be detected after transaction is done. It is difficult to find out fraudulent and regarding losses will be barred by issuing authorities. Hidden markov mode is the statistical tools for engineers and scientists to solve various problems. Credit card fraud can be detected using hidden markov model during transactions. Hidden markov model aids to obtain a high fraud transaction coverage combined with low false alarm rate, thus providing a better and convenient way to detect frauds. Using hidden markov model, customer's pattern is analyzed and any deviation from the regular pattern is considered to be a fraudulent transaction. So in our project we will be using hidden markov model to detect fraudulent transaction.

Keywords: Hidden markov model, fraud transaction, Credit card, online shopping, fraud detection.

INTRODUCTION

In everyday life credit cards are used for purchasing goods and services using online transaction or physical card for offline transaction. In credit or debit card based purchase, the cardholder presents his card to a merchant for making payment. To make fraud in this kind of acquisitions, the person doing fraud has to steal the credit card. If the legitimate user does not understand the loss of card, it can lead to important financial loss to the credit card company and also to the user.

In online payment mode, attackers need only little information for doing false transaction example secure code, expiration date, card number and many other factors. In this purchase method, mainly transactions will be done through Internet or telephone. To obligate fraud in these types of purchases, an impostor simply needs to know the card details. Most of the time, the honest 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 analyse the spending patterns on every card and to figure out any irregularity with respect to the "usual" spending patterns. Fraud discovery based on

the examination of existing purchase data of cardholder is a likely way to reduce the rate of positive credit card frauds. Since humans tend to display specific behaviourist profiles, every cardholder can be characterized by a set of patterns comprising information about the distinctive purchase category the time since the last buying, the amount of money spent, and other things. Nonconformity from such patterns is reflected as fraud.

**CREDIT CARD FRAUD DETECTION
USING HMM**

In scheduled system, by using Hidden Markov Model (HMM) this does not require fraud signatures and yet is able to detect frauds by considering a cardholder's expenditure habit. Card transaction processing sequence by the stochastic process of an HMM. The details of items bought during the transactions are usually not known to an FDS running at the bank that issues credit cards to the user. Therefore HMM is a perfect choice for addressing this issue. To finish the transaction user should response to the security questions. The fraud is established by querying the

user with some security code which is sent by email transaction which is proceed only when verification code is correct otherwise transaction is cancelled. Fraud is sensed using the probability difference that is in between old observation sequence and new observation sequence.

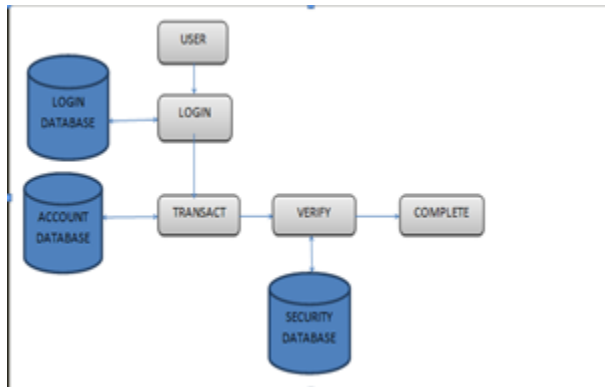


Fig 1. Outline of proposed system

The system of credit card fraud detection based on Hidden Markov Model, which does not involve fraud signatures and still it is clever to detect frauds just by keeping in mind a cardholder's spending habit. The particulars of purchased items in single transactions are generally unidentified to any Credit card Fraud Detection System running either at the bank that issues credit cards to the cardholders or at the merchant site where goods is going to be purchased.

As business processing of credit card fraud detection system runs on a credit card supplying bank site or merchant site. Each incoming transaction is submitted to the fraud detection system for confirmation purpose. The fraud detection system is programmed to accept the card details such as cvv number, credit card number, card type, expiry, the amount of items purchase to authenticate and date to verify whether the transaction is real 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 expenditure profile of cardholder. The number of items bought, types of items that are bought in a certain transaction are not known to the Fraud Detection system, but it only focuses 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 series.

It tries to find out any alteration in the transaction based on the spending behavioural profile of the cardholder, shipping address, and billing address and various other factors. The probabilities of initial set have been chosen based on the spending behavioural profile of card holder and a sequence for more processing of information is constructed. If the fraud detection system decides that the transaction to be is of fake nature, it gives an alarm, and the providing bank declines the transaction.

For the security purpose, the Security information constituent will get the information features and will store it in database. If the card lost then the Security information module form ascends to accept the security information. The security form has a number of security questions likemother name, account number, date of birth, other personal question and their reply, etc. where the user has to answer it correctly to move to the transaction section. All these evidence must be known by the card holder only. It has informational privacy and informational self-determination that are addressed evenly by the innovation affording people and entities a trusted means to user, secure, search, process, and argument personal and/or confidential information.

The system and tools for pre-authorizing business provided that a connections tool to a seller and a credit card owner. The cardholder inductees a credit card transaction processing by communicating to a credit card number, card type with expiry date and storing it into database, a distinctive piece of information that characterizes a particular transaction to be made by an authoritative user of the credit card at a later time.

The details are received as network data in the database only if an accurate individual acknowledgement code is used with the communication. The cardholder or other imposing user can then only make that particular transaction with the credit card. Since the transaction is pre-authorized, the vendor does not need to see or diffuse an accurate individual recognition code.

The diagram that follows shows the flowchart of the Hidden Markov Model implementation and how the control of the system will transfer will take place from one place to another.

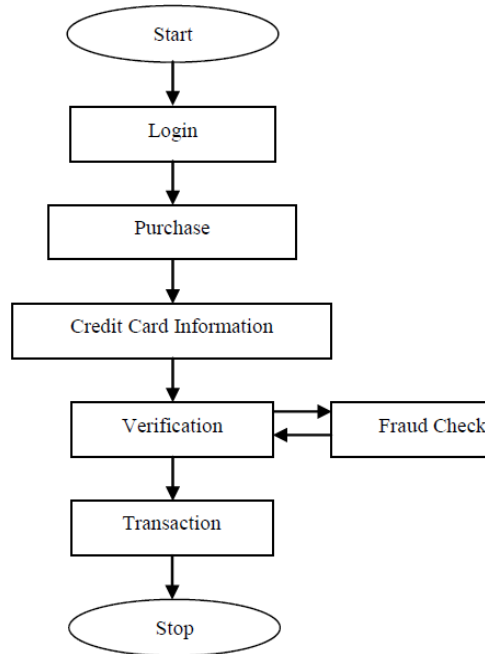


Fig.2: Flowchart of HMM implementation

HMM BACKGROUND

An HMM has a determinate set of states ruled by a set of transition possibilities. In a specific state, an outcome or observation can be created according to a related probability distribution. It can be used to model much more complex stochastic procedures as compared to an old-style Markov model.

HMM-based applications are mutual in various areas such as speech recognition, bioinformatics, and genomics.

In recent years, Joshi and Phoba [8] have investigated the capabilities of Hidden Markov Model in anomaly detection. They classify TCP network traffic as an attack or normal using HMM.

Cho and Park [9] suggest an HMM-based intrusion detection system that improves the modelling time and performance by considering only the privilege transition flows based on the domain knowledge of attacks.

Ourston et al. [10] have proposed the application of HMM in detecting multistage network attacks.

Hoang et al. [11] present a new method to process sequences of system calls for anomaly detection using HMM. The key idea is to build a multilayer model of program behaviours based on both HMMs and enumerating methods for anomaly detection.

Lane [12] has used HMM to model human behaviour. Once human behaviour is correctly modelled, any detected deviation is a cause for concern since an attacker is not expected to have behaviour similar to the genuine user.

OTHER TECHNIQUES TO CHECK CREDIT CARD FRAUD DETECTION

Ghosh and Reilly [4] have proposed a neural network technique to identify credit card scam transaction. They have constructed a detection system, which is proficient on a large sample of credit card account transactions. These examples contain cases due to stolen cards, lost cards, application fraud, lifted card details, forged fraud etc. They verified on a data set of all dealings of credit card account over a valid period of time.

Credit card fraud detection has received an important attention from researchers in the world. Several techniques have been developed to detect fraud transaction using credit card which are based on data mining, clustering techniques, neural network, genetic algorithms, decision tree, Bayesian networks [5] and many more.

Bayesian networks are also one technique to detect fraud [6]. These techniques produce better results but having large cycle time to identify fraud. But the time restraint is one main drawback of this technique, exclusively when compared with neural networks.

Another technique that has been suggested by Bentley [1] is constructed on genetic programming. A Genetic algorithm is used to create logic rules capable of classifying credit card transactions into suspicious and non-suspicious classes. Basically, this method follows the recording process in which unsettled payment was checked against last three month payment. If it is greater than that of last three month, then it will be considered as doubtful or else it will not be doubtful.

Concept of similarity tree using decision tree logic is also used to detect frauds which are easy to implement and understand but disadvantage is it takes a long time to process request.

Clustering algorithm is also used to detect fraud. In this technique, clustering of two algorithms have used for behavioural fraud detection.

Data mining technique is also used to detect fraud but this technique is very time consuming and tedious to implement.

ALGORITHMS USED

To record the credit card transaction indulgence process in conditions of a Hidden Markov Model (HMM) [7], it creates through original deciding the inspection symbols in our representation. We quantize the buying values x into M price ranges V_1, V_2, \dots, V_M , form the study symbols by the side of the issuing bank. The genuine price variety for each symbol is configurable based on the expenditure routine of personal cardholders. HMM determine these prices rang dynamically by using clustering algorithms (like K clustering algorithm) [3] on the price values of every card holder transactions. It uses cluster V_k for clustering algorithm as $k = 1, 2, \dots, M$, which can be represented both observations on price value symbols as well as on price value range.

In this prediction process it considers mainly three price value ranges such as 1) low (l) 2) Medium (m) and 3) High (h). So set of this model prediction symbols is $V = \{l, m, h\}$, so $V = \frac{1}{4}$ as l (low), m (medium), h (high) which makes $M = \frac{1}{4} \times 3$. E.g. If card holder perform a transaction as \$ 250 and card holders profile groups as l (low) = (0, \$ 100], m (medium) = (\$ 200, \$500], and h (high) = (\$ 500, up to credit card limit], then transaction which card user want to perform will come in medium group. So the corresponding profile group or symbol is M and V (2) will be used.

In several period of time, acquisition of various types with the varied amount would be made by credit card holder. It utilizes the deviation recorded in the purchasing amount of last 10 transaction sequence (and adding one new transaction in that sequence) which is one of the possibilities linked to the probability calculation.

In the beginning stage, model does not have data of last 10 transactions, in that case, model will ask to the cardholder to feed basic information during transaction about the user. Due to feeding of information, HMM model acquired relative data of transaction for further verification of transaction on spending profile of cardholder.

ADDITIONAL SECURITY FEATURES

Along with using the HMM algorithm for detection of frauds we have implemented additional features like internet IP address tracking and shipping address is also verified and checked for additional security.

In internet IP address detection, the information related to the IP address of the area in which the user is currently residing during making the transaction is stored in the database. This provides the database with the area location of the user and stores it. The information is cross checked every time the user makes a purchase online using the credit card and if any anomaly is detected then fraud detection system gets activated and necessary steps are taken to ensure the user is legitimate.

In shipping address detection system the shipping address of the user is stored in the database for future references and every time the user makes a purchase the shipping address is also cross checked for enhanced verification and security purposes. The address on which the user usually orders things is stored in this method and is cross checked every time when the user makes a request or orders anything.

ADVANTAGES AND DISADVANTAGES

Credit card fraud detection using the HMM algorithm along with MAC address and shipping address is very useful and efficient in solving the frauds related to credit card and thus prevents frauds and gives enhanced security and protection against online frauds.

Advantage of HMM algorithm is the detection of the fraud use of the card is found much faster than the existing system.

In case of the existing system even the original card holder is also checked for fraud detection. But in this system if the user is proven to be legitimate then no need to check the original user.

The user information log which is maintained will be used by the bank as a proof for the bank for the transaction made by the user.

We can find very accurate fraud detection using this technique thus enhancing the results.

This reduces the burden and work of an employee in the bank as they don't have to manually enter the data or check for frauds.

The Hidden Markov Model makes the task of detection of frauds very easy and also helps to remove the complexity.

It does not require fraud signatures.

Disadvantages are very limited and the only disadvantage in our system is that we need to observe the first 10 transaction and then the software starts calculating and detecting the fraud transaction.

APPLICATION

1. Provide easy and well security to Online Shopping
2. Detect Frauds and trace the Location from wherethe transaction has been made.

RESULTS AND DISCUSSIONS

In this part, it is shown that fraud detection will be based on last 10 transactions and also calculate percentage of each spending profile (low, medium and high) based on total number of transactions. In the table given below (Table 1), list of all transactions are shown.

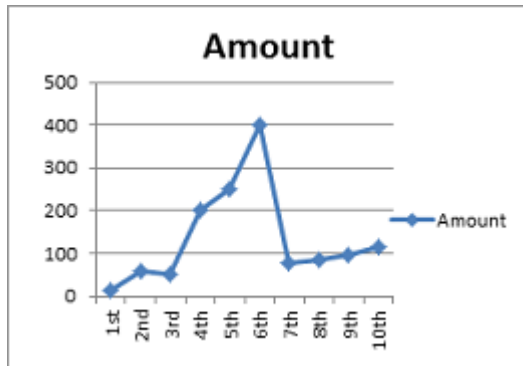


Fig2. Spending profile of all transaction

The percentage calculation of each spending profile (low, medium and high) of the card holder based on price distribution range as mentioned earlier is shown in Figure 3.

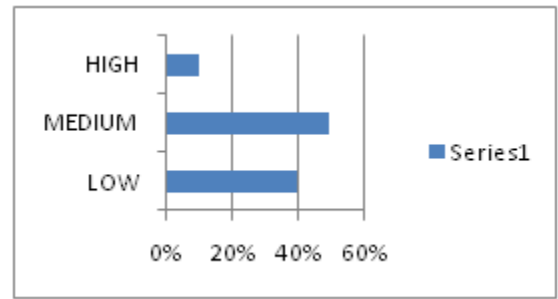


Fig 3. Percentage of each spending profile.

It has been observed from the table above that medium spending profile has maximum percentage of 45, followed by low profile 40% and then 15% of high spending profile as per details of transactions in Table (table 1).

Table 1

No_of_transaction	Amount
1 st	150
2 nd	60
3 rd	50
4 th	200
5 th	250
6 th	400
7 th	79
8 th	85
9 th	95
10 th	115

CONCLUSION

It has been discussed in this paper, that how Hidden Markov

Model will enable to end false online transaction through credit card. The Fraud Detection System is also accessible for controlling vast volumes of transactions handling. The HMM based credit card fraud detection system is not taking much time and in spite of having difficult process to achieve fraud check like the present system and it gives better and fast result. The Hidden Markov Model makes the handling of detection very easy and tries to eliminate the complexity.

We recommended system which is an application of Hidden Markov Model in Anomaly or fraud detection. The diverse steps in credit card transaction handling are represented as the essential method of an HMM. The system implemented takes all the user information and deals with the data carefully to detect

online frauds. It has also been described how they can detect whether an inbound transaction is fraudulent or not. Additional security features like MAC address detection and also shipping address verification are provided for enhanced security and better detection of fraud transaction. This proposed method can be made more advanced and better version can be developed and enhanced in the future.





REFERENCES

1. Bentley, Peter J., Kim, Jungwon, Jung, Gil-Ho and Choi, Jong-Uk, (2000) "Fuzzy Darwinian Detection of Credit Card Fraud", Proc. of 14th Annual Fall Symposium of the Korean Information Processing Society
2. Chiu,C., and Tsai, C.,(2004) . A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection.Proceedings of IEEE international conference e-technology, e-commerce and e-service(2004).
3. Fan, W., Prodromidis, A, L., and Stolfo, S.J., 1999.Distributed Data Mining in Credit Card Fraud Detection.IEEE intelligent system, vol 14, no.6 (1999).
4. Ghosh, Sushmito& Reilly, Douglas L., (1994) "Credit Card Fraud Detection with a Neural-Network",Proc. of 27th Hawaii Int'l Conf. on System Science: Information systems: Decision Support and Knowledge-Based Systems, Vol.3, pp. 621-630.
5. Maes, Sam, Tuyls Karl, Vanschoenwinkel Bram &Manderick, Bernard, (2002) "Credit Card Fraud Detection Using Bayesian and Neural Networks", Proc. of 1st NAISO Congress on NeuroFuzzyTechnologies.Hawana.
6. SonaliN.Jadhav,KiranBhandari-Anomaly Detection using Hidden Markov Model.
7. V.Bhusari and S.patil.Study of Hidden Markov Model in Credit Card Fraudulent Detection.
8. S.S. Joshi and V.V. Phoha, "Investigating Hidden Markov Models Capabilities in Anomaly Detection," Proc. 43rd ACM Ann. Southeast Regional Conf., vol. 1, pp. 98-103, 2005.
9. S.B. Cho and H.J. Park, "Efficient Anomaly Detection by ModelingPrivilege Flows Using Hidden Markov Model," Computer andSecurity, vol. 22, no. 1, pp. 45-55, 2003.
10. D. Ourston, S. Matzner, W. Stump, and B. Hopkins, "Applications of Hidden Markov

Models to Detecting Multi-Stage NetworkAttacks," Proc. 36th Ann. Hawaii Int'l Conf. System Sciences, vol. 9,pp. 334-344, 2003.

11. X.D. Hoang, J. Hu, and P. Bertok, "A Multi-Layer Model forAnomaly Intrusion Detection Using Program Sequences of SystemCalls," Proc. 11th IEEE Int'l Conf. Networks, pp. 531-536, 2003.
12. T. Lane, "Hidden Markov Models for Human/Computer InterfaceModeling," Proc. Int'l Joint Conf. Artificial Intelligence, Workshop Learning about Users, pp. 35-44, 1999.

Author Bibliography

	<p>Ashish Thakur Received the H.S.C. degree in Science from Airforce School, Pune in 2011. During 2011-2015, he completed his B.E. (I.T.) from Sinhgad Academy of Engineering, Pune.</p>
	<p>Vinita Jain Received the H.S.C. degree in Science from NowrosjeeWadia College, Pune. During 2011-2015, she completed her B.E. (I.T.) from Sinhgad Academy of Engineering, Pune.</p>
	<p>Bushra Shaikh Received the H.S.C. degree in Science from AKI's Poona College, Pune in 2011. During 2011-2015, she completed her B.E. (I.T.) from Sinhgad Academy of Engineering, Pune.</p>
	<p>A.M. Magar He is Assistant Professor at Department of Information Technology, SAE, Kondhwa.</p>