ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 3, March 2015*

# Credit Card Fraud Detection using Hidden Markov Model

**AashleshaBhingarde[1], AvnishBangar[2], Krutika Gupta[3], SnigdhaKarambe[4]**

Department of Information Technology P.V.P.P College of EngineeringSion, Mumbai[1,2,3,4]

**Abstract:** The most accepted payment mode is credit card for both online and offline in today's world, it provides cashless shopping at every shop in all countries. It will be the most convenient way to do online shopping, paying bills etc. Hence, risks of fraud transaction using credit card has also been increasing. In the existing credit card fraud detection business processing system, fraudulent transaction will be detected after transaction is done. It is difficult to find out fraudulent and regarding loses will be barred by issuing authorities. Hidden Markov Model is the statistical tools for engineer and scientists to solve various problems. In this paper, it is shown that credit card fraud can be detected using Hidden Markov Model during transactions. Hidden Markov Model helps to obtain a high fraud coverage combined with a low false alarm rate.

**Keywords**: Internet, online shopping, credit card, e-commerce security, fraud detection, Hidden Markov Model**.**

## I. INTRODUCTION

In day to day life credit cards are used for purchasing goods and services with the help of virtual card for online transaction or physical card for offline transaction. In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. 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 to the credit card company. In online payment mode, attackers need only little information for doing fraudulent transaction (secure code, card number, expiration date etc.).

In this purchase method, mainly transactions will be done through Internet or 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. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful credit card frauds. Since humans tend to exhibit specific behaviouristic profiles, every cardholder can be represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system.

## II. HIDDEN MARKOV MODEL

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 set 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" 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:

1) Low (l),
2) Medium (m) and,
3) 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. APPLICATION DESCRIPTION

In existing models, the bank is verified credit card information, CVV number, Date of expiry etc., but all these information are available on the card itself. Nowadays, bank is also requesting to register your credit card for online secure password. In this new model, after feeding details of card at merchant site, then it will transfer to a secure gateway which is established at bank's own server. But, it is not verifying that the transaction is fraudulent or not. If hackers will get secure code of credit card by phishing sites or any other source, then it is very difficult to trace fraudulent transaction. In proposed model based on HMM will help to verify fraudulent of transaction during transaction will be going to happen. It includes two modules are as follow

## IV. ONLINE SHOPPING

It comprises with many steps, first 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

DOI 10.17148/IJARCCE.2015.4341

these information, now the page will be directed to proposed fraud detection system which will be installed at bank's server or merchant site.

## V. FRAUD DETECTION SYSTEM

All the information about credit card (Like Credit card number, credit card CVV number, credit card Expiry month and year, name on credit card etc.) will be checked with credit card database. If User entered database is correct then it will ask Personal Identity number (PIN). After matching of Personal Identity number (PIN) with database and account balance of user's credit card is more than the purchase amount, the fraud checking module will be activated.

The verification of all data will be checked before the first page load of credit card fraud detection system. If user credit card has less than 10 transactions then it will directly ask to provide personal information to do the transaction. Once database of 10 transactions will be developed, then fraud detection system will start to work. By using this observation, determine users spending profile.

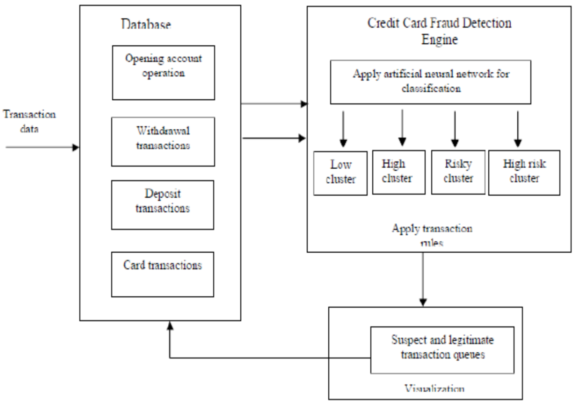
The purchase amount will be checked with spending profile of user. By transition probabilistic calculation based on HMM, it concludes whether the transaction is real or fraud. If transaction may be concluded as fraudulent transaction then user must enter security information. This information is related with credit card (like account number, security question and answer which are provided at the time of registration).

If transaction will not be fraudulent then it will direct to give permission for transaction. If the detected transaction is fraudulent then the Security information form will arise. It has a set of question where the user has to answer them correctly to do the transaction. These forms have information such as personal, professional, address; dates of birth, etc are available in the database.

If user entered information 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.

## VI. SYSTEM ARCHITECTURE

The implemented architecture consists of two subsystems: database interface and credit card fraud (CCF) detection engine. The database interface subsystem is the entry point through which the transactions are read into the system. It is the system's interface with the banking software. Visual Basic.Net was used for the design of CCF detection, that is, as a front-end while Microsoft Access was used for the design of training and test database, as back-end. In the CCF detection subsystem, each transaction entering into the system was passed to the host server where the corresponding transaction profile is further checked using neural networks and transactions business rules.



Fig(1):System Architecture

## VII. SUMMARY

Established connection between the database and web application. We have effectively implemented the first phase of our credit card fraud detection model. Admin login form is created successfully with the commencement of admin session and termination after logout

## VIII. FUTURE SCOPE

The future work on which we are focusing now is to implement and measure the performance of our proposed system so that we can justify that our proposed system is better in credit card fraud detection then all the previous proposed system.

## REFERENCES

[1]. P. Chan and S. Stolfo, "Metalearning for Multistrategy and Parallel Learning," Proc. SecondInt'l Workshop Multistrategy Learning, Center for Artificial Intelligence, George Mason Univ., Fairfax,Va., 1993, pp. 150–165.

[2]. S. Stolfo et al., "JAM: Java Agents for Metalearning over Distributed Databases," Proc.Third Int'l Conf. Knowledge Discovery andData Mining, AAAI Press, Menlo Park, Calif., 1997, pp. 74–81.

[3]. D. Wolpert, "Stacked Generalization," Neural Networks,Vol. 5, 1992, pp. 241–259.

[4]. P. Chan and S. Stolfo, "Toward Scalable Learning with Nonuniform Class and Cost Distributions: A Case Study in Credit Card Fraud Detection," Proc. Fourth Int'l Conf.Knowledge Discovery and Data Mining, AAAI Press, Menlo Park, Calif., 1998, pp. 164–168.

[5]. Lijun Cao, Xiyin Liu, TiejunZhou ,Zhongping Zhang Aiyong Liu; Based on the flow of anti-k nearest neighbors algorithm for data mining outliers; In Proceedings of IC-BNMT2010

[6]. Yufeng Kou, Chang-Tien Lu, SiriratSinvongwattana ,Yo-Ping Huang; Survey of Fraud Detection Techniques; in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control Taipei, Taiwan, March 21-23, 2004

[7]. Y. Dora Cai, David Clutter, Greg Pape, Jiawei Han. MAIDS; Mining alarming incidents from data streams; In SIGMOD, Paris,2004:919-920

[8]. Charu C. Aggarwal, Philip S. Yu; An effective and efficient algorithm for high-dimensional outlier detection; In The VLDBJournal (2005) 14: 211–221

[9]. [5] AleksandarLazarevic, Vipin Kumar; Feature Bagging for Outlier Detection; In Proceedings of KDD'05, August 21–24, 2005,

DOI 10.17148/IJARCCE.2015.4341