Credit Card Fraud Detection Using Hidden Markov Model

Snehal J. Patil¹, A. S. Dange²

Department of Computer Science & Engineering
AnnasahebDange College of Engineering & Technology, Ashta, Shivaji University, Kolhapur, India

Abstract:
The objective is to make secure mechanism to detect credit card crimes, more precisely to identify replica in credit card. It is important to establish techniques for detecting and preventing credit card fraud. However, there are various parameters that need to be considered before deciding which technique best suits the needs of a particular situation. A technique, i.e. Hidden Markov Model promises a high predictive accuracy used in the fraud detection system. This research is totally related to credit card application fraud detection by performing the process of asking security queries to the persons involved in the transactions, by checking probability of transactions. Although the use of credit cards as payment method can really convenient for our daily transactions; people must be aware of the risks so they impose themselves when using their credit cards. More precisely the incremental usage of credit cards gave the opportunity for fraudsters to exploit their vulnerabilities.

Keywords: Credit card, online shopping, fraud detection, hidden Markov Model

I. INTRODUCTION

Credit card fraud is defined as Unauthorized account activity by a person for which the account was not intended. Fraud detection involves to identifying Fraud as quickly as possible once it has been perpetrated. Banking system provides e-cash and e-commerce as well as e-services improving for online transaction. Credit card is one of the most conventional ways of online transaction. In the case of risk of fraud transaction using credit card has also been increasing. Credit card fraud detection is one of ethical issues in the credit card companies, mortgage companies, banks and financial institutes. Credit card fraud is most common and costly crime in existencethese days [1]. Many types of known fraud matching methods were used in existing system to detect frauds. However, all these methods have certain limitations. A new detection system is being proposed which find fraudster. This research is totally concerned with credit card application fraud detection is performing the process of asking security queries and by checking probabilities of previous andcurrent transactions to the person involved in the transaction.

II. LITERATURE SURVEY

AlkaHerenj and Susmita Mishra et al describe the “Secure mechanism for Credit card transaction fraud detection system”, [1]. In this paper, the model is totally concerned with credit card application fraud detection by performing the process of asking security queries to the persons involved in the transactions and as well as by removing real time data errors. Linda Delamaire, Hussein Abdou and John Ppointonet al describe the “Credit card fraud and detection techniques”, [2]. In this paper, The main aim is to identify the different types of credit card fraud and to review alternative techniques that have been used in fraud detection. Krishna Kumar Tripathi and Mahesh A. Pavaskar et al describe the “Survey on credit card fraud detection techniques”, [3]. In this paper, presents a survey of various techniques used in credit card fraud detection mechanism. AkkiniSriranjani and Dr. Syed Sadat Ali et al describe the “Methods oriented with detection of fraud based on credit card analysis”, [4]. In this paper the experiments are conducted on the present method where it effectively improves the performance of the system in a well effective manner.

III. MOST IMPORTANT CHALLENGES DESIGNED FOR DETECTION SYSTEMS ARE

The two most advanced challenges for data mining based layers of defense are adaptively and quality data. These challenges want to be addressed in order to condense fake positives. Adaptively accounts for morphing rip-off behavior, as the challenge to observe fraud changes itsbehavior. But what is not noticeable, however equally essential, is the need to also account for unstable legalbehavior enclosed by a changing environment. In the credit application domain, varying legal behavior exhibited by communal relationships furthermore it can be caused by peripheral events. This way authorized behavior can rigid to decide from fraud behavior. The detection system requests to work out carefulness by means of applications which reproduce communal relationships. It also needs to make allowance for certain peripheral actions. Quality data are tremendously attractive for data mining along with data quality can be enhanced allthe way through the real time removal of data errors. The detection system has to clean duplicateswhich have been reentered due to human error or else for other reasons. It also desires to disregard unnecessary attributes which have numerous missing values, as well as additional issues.

IV. CREDIT CARD FRAUD

Application Fraud: In the application fraud when someone is applies for credit card with false information that is termed as application fraud. For detecting the application fraud, two different situations have to be classified. When applications come from same user with same details, that is called duplicates, and when applications come from different individuals with similar details, that is called as identity fraudsters.

Theft Fraud/Counterfeit Fraud: Theft fraud refers using a card that is not yours. As well as the owner give some feedback and contact the bank, the bank will take measures to
check the thief as early as possible. Likewise, the counterfeit fraud occurs when the credit card is used remotely; where only the credit card details are needed.

**Account Takeover**: This type of fraud occurs when a fraudster illegally obtains the valid customers personal information. The fraudster takes control of (takeover) a legitimate account by providing the customer’s account number or by providing the card number.

**Skimming**: Most cases of counterfeit fraud involve skimming, a process where real data on a card’s magnetic stripe is electronically copied onto another. Skimming is fast emerging as the most popular form of credit card fraud.

**Stolen and counterfeit** cards together contribute to more than 50% of fraud. Credit card is used by both purpose for online or offline transaction, mostly credit card is divide two brought categories, first is physical credit card, now in the physical credit card where card holder is present, which is relation between the selling counter and the card holder. The Selling counter can use the EMV (Europay, MasterCard, and visa) machine. Transaction of the amount is done in front of the card holder. Virtual credit card is where card holder in not present, an internet baking is part of the virtual credit card. Online baking is challenging part of traditional banking system. The credit card is use of the modern society day by day. Prevalent of the credit card fraud is difficult task when using online transaction.

**V. CREDIT CARD FRAUD DETECTION USING HMM**

Hidden Markov Model (HMM) is does not require fraud signatures and yet is able to detect frauds by considering a cardholder’s habit. Credit card transaction processing sequence by the stochastic process of Hidden Markov Model. The details of the items bought during the transactions are usually not known to an FDS running at the bank that issues credit cards to user. Since HMM is a perfect choice for addressing this issue. To finish the transaction user should response to the security questions. The fraud established by querying the user with some security code which is sent by email transaction is proceed if verification code is correct otherwise transaction it is cancelled. Fraud is sensed using probabilities difference that in between old observation sequence and new observation sequence.

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

As the business processing of the credit card fraud detection system runs on the credit card supplying bank site or merchant site. Every incoming transaction is properly submitted to the fraud detection system for confirmation purpose. The fraud detection system is programmed to accept the card details such as Card Verification Value (cvv) number, credit card number, card type, expiry, the amount of the items purchase to authenticate and date to verify whether the transaction is real or not.

The implementation techniques of the Hidden Markov Model in order to detect fraud transaction through credit cards, it makes the groups of training set and to identify the spending profile of cardholder. The number of items bought, types of an items that are bought in a certain transaction they are not known to the Fraud Detection system, but it only focuses on the amount of an item purchased and use for further processing. It stores data of different amount of transactions in form of the clusters depending on transaction amount which will be either in low, medium or high value series.

It is tries to find out the any alteration in the transaction based on the spending behavioral profile of the cardholder, shipping address, billing address and any various other factors. The probabilities of initial set have been chosen based on the spending behavioral profile of the card holder and a sequence for more processing of information is constructed. If fraud detection system is known any transaction is fake, then it gives an alarm and the providing bank stop the transaction. For the purpose of security, the Security information constituent will get the information data that is store in the database. If any case the card is lost then the Security information module form ascends to accept security information. The security information form has a number of security questions like mothers name, account number then date of birth and other personal questions and their reply, etc. where the user has to answer is correctly then move to the transaction section. All these answers must be known by the card holder only. It has data privacy and an informational autonomy that are addressed evenly by an improvement affording people and entities a trusted means to user, secure, search, process, and an argument personal and/or confidential information.

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

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

**VI. MODEL DESCRIPTION**

In the existing models, the bank is verified the credit card information, CVV number, Date of expiry etc., but all these information are available on the credit card itself. Nowadays, bank is also requesting to register your credit card for online secure password. In this model, after feeding details of credit card at merchant site, then it will transfer to a secure gateway is established at the bank’s own server. But, it is not verifying that the transaction is fraudulent or not. If hackers will get secure code of the credit card by phishing sites or any other source, then it is very difficult to trace fraudulent transaction.

In the proposed model it is based on HMM will help to verify fraudulent of transaction during transaction is happen.
It includes two modules are as follow:

I] Online Shopping
In the online shopping it comprises many steps, first is to login into a particular site to purchase goods or services, then choose an item and next step is go to payment mode where credit card information will be required. After filling all these information, now the page is directed to proposed fraud detection system which will be installed at bank’s server or merchant site.

II] Fraud Detection System
In fraud detection system all the information about credit card will be checked with credit card database. If User entered the database is correct then it will ask the Personal Identity number (PIN). After matching of Personal Identity number (PIN) with the database and an account balance of the user’s credit card is more than the purchase amount, the credit card fraud checking module will be activated Then the verification of all data will be checked out before the first page is load of the credit card fraud detection system.

In case of user credit card has less than 10 transactions then it is directly ask to provide the personal information to do the transactions. Once database of 10 transactions is developed, then fraud detection system will start to work.

After that by using this observation, determines users spending profile. The purchase amount is checked with spending profile of the user. By transition probabilistic calculation based on the HMM, where it concludes whether the transaction is real or fraud. If the transaction may be concluded as fraudulent then user must be enter security information. This information is related with the credit card (like account number, security questions and answers which are provided at the time of registration). If the transaction will not be fraudulent then it is direct to give permission for transaction.

In the case of detected transaction is fraudulent then Security information form will arise. It has a set of question where the user has to must answer them correctly to do the transaction. These forms havean information such as personal or professional address and dates of birth etc are available in the database. If user entered an information will be matched with database information, then the transaction will be done securely. And else the user transaction will be terminated and transferred to the online shopping website. The flowchart of proposed module is shown in Figure 1.

![Flowchart of HMM module for credit Card fraudulent detection](image)

**Fig1:** Flowchart of HMM module for credit Card fraudulent detection

---

VII. CONCLUSION

The main focus is the detection of fraudsters in credit applications and by implementing the new data mining layers which helps in performing a secure transaction. It has documented the development and evaluation in credit card application fraud detection system. In this survey the various approaches towards credit card fraud detection is been overviewed and a brief discussion of Hidden Markov Model (HMM) 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.

VIII. FUTURE WORK

In future work we adaptive Communal Analysis Suspcion Scoring (CASS) algorithm to observe application streams to detect the changing attack patterns which are in direct reply to our existing search parameters.

In future work of the findings obtained here may not be generalized to the global fraud detection problem. As future worksome effective algorithm which can be perform well for the classification problem with variable miss classification costs could be developed.

In future work we can prepare an application with consistent Fraud Detection with new techniques and modules, develop a sophisticated module like calculating Fraud Timings, capturing the photo of the Fraud and many more modules can be developed.

XI. REFERENCES


