Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Hidden Markov Model in Credit Card Fraud Detection

Ashish Thakur, Bushra Shaikh, Vinita Jain, A. M. Magar
I T & SP Pune University, Pune,
Maharashtra, 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 analysed 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

I. INTRODUCTION

When In everyday life credit cards are used for purchasing goods and services using online transaction or physical card for offline transaction. In physical-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.

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 analyze 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 behaviorist 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.

II. RELATED WORK ON 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 example 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 behavioral fraud detection.

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

III. 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 Hidden Markov Model. 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 probabilities difference that is in between old observation sequence and new observation sequence.

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 makes groups of training set and identify the spending 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 behavioral 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 behavioral 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 like mothers 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 proof must be known by the card holder only. It has data privacy and informational autonomy that are addressed evenly by the improvement 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 induces a credit card transaction processing by communicating to a credit card number, card type with expiry date and storing it into database, a unique piece of data that characterizes a particular transaction to be made by an trustworthy 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.

IV. USE OF HMM FOR CREDIT CARD FRAUD DETECTION

A fraud detection system (FDS) runs at a credit card issuing bank. Each inward transaction is given to the FDS for verification. FDS obtains the card details and the worth of purchase to confirm whether the transaction is genuine or not. The types of products that are bought in that transaction are not known to the FDS. It attempts to find any irregularity 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 fake, it detects an intrusion, and the issuing bank declines the transaction. The concerned card holder 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.

A. HMM Model for Credit Card Transaction Processing

To draw the credit card transaction handling operation in terms of an HMM, we start by first determining the observation symbols in our model. We quantize the purchase values x into M price ranges V1; V2; . . . VM, establishing the observation symbols at the allotting bank.

B. Generation of Observation Symbols

For each cardholder, we train and keep an HMM. To find the observation symbols corresponding to individual cardholder's transactions dynamically, we run a clustering algorithm on his past transactions. Normally, the transactions that are stored in the issuing bank's database contain many attributes.

C. Checking spending Profile

The spending profile of a cardholder proposes his normal spending performance. Cardholders can be generally categorized into three groups based on their spending habits, namely, high-spending group, medium-spending group, and low-spending group.

D. Model Parameter Estimation and Training

The model is trained for the first 10 transaction so that it is able to effectively detect the frauds. Using this technique makes the system to develop the data for future references so that the fraud is detected effectively in the future and no discomfort is caused to the user.

E. Fraud Detection

After the HMM factors are learned, we take the symbols from a cardholder's training data and form an initial sequence of symbols.

V. ALGORITHM USED

To record the credit card transaction indulgence process in conditions of a Hidden Markov Model (HMM), it creates through original deciding the inspection symbols in our representation. We quantize the buying values x into M price ranges V1, V2 . . . VM, 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) on the price values of every card holder transactions. It uses cluster Vk for clustering algorithm as k ¼ 1, 2 . . . . 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 ¼ f as l (low), m (medium), h (high) which makes M ¼ 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 holder want to do will come in medium profile group. So the corresponding profile group or symbol is M and V (2) will be used.

In various period of time, purchase of various types with the different amount would make by credit card holder. It uses the deviation in a purchasing amount of latest 10 transaction sequence (and adding one new transaction in that sequence) which is one of the possibilities related to the probability calculation.

In initial 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 cardholder such as mother name, place of birth, mailing address, email id etc. Due to feeding of information, HMM model acquired relative data of transaction for further verification of transaction on spending profile of cardholder.

VI. CONCLUSION

We recommended system which is an application of HMM in Anomaly Detection. The diverse steps in credit card transaction handling are represented as the essential method of an HMM. Suggested system recommends a process for finding the spending profile of cardholders, as well as submission of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It has also been described how they can detect whether an inbound transaction is fraudulent or not. Additional security features like internet IP address detection and also shipping address verification are provided for enhanced security and better detection of fraud transaction. This proposed method can be 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

AUTHOR PROFILE

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.

BushraShaikh 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.

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.

A.M. Magar, Assistant Professor, Department of Information Technology, SAE, Kondhwa.

