ISSN:0975-9646

Gaurav Mhatre et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2053-2055

Credit Card Fraud Detection Using Hidden Markov Model

Gaurav Mhatre , Oshan Almeida , Dhiraj Mhatre ,Poonam Joshi

[#]*Information technology Department, Mumbai University,Atharva college of Engineering, Malad (w), Mumbai-400095, Maharashtra, India*

***Abstract*— The Internet has taken its place beside the telephone and the television as an major part of people's day-to-day lives. Consumers rely on online shopping and banking. Most online shoppers use credit cards to pay for their purchases. As credit card becomes the most popular mode of payment, cases of fraud associated with it are also increasing. In this paper, we model the sequence of operations in credit card transaction processing using a Hidden Markov Model (HMM) and show how it can be used for the detection of frauds. An HMM is trained with normal behavior of cardholder. If an incoming credit card transaction is not accepted by the HMM with sufficiently high probability, it is considered to be fraudulent. We present detailed experimental results to show the effectiveness of our approach.**

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

I. INTRODUCTION

Credit-card-based purchases can be categorized into two types: 1) physical card and 2) virtual card. In a physical-card based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraud 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 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. 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 behaviorist 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. RELATED WORK

A.Fraud Detection System [1]

All the information about credit card Like Credit card number,name,cvv number, Expiry month and year of credit card ect. Checked credit card database. When user is enter the correct information then it will ask Personal Identity number (PIN). Then system is matching of Personal Identity number (PIN) with given account information, the fraud checking module will be activated.when we load the first page of credit card fraud detection system it start the verification 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, then it decided transaction is real or fraud if the transaction is fraudulent transaction then system will asked some 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 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. The flowchart of proposed module is shown in Fig 1(a)

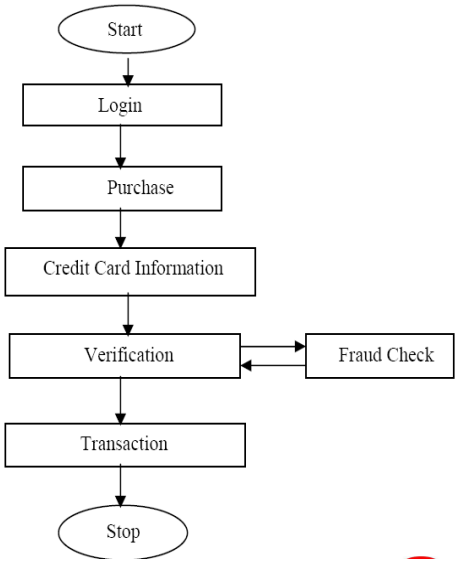

Fig: 1 *Flowchart of HMM module for credit Card fraudulent detection*

III. CLASSIFICATION TECHNIQUES

A.Neural networks

Neural network is defined as a set of interconnected nodes designed to represent functioning of the human brain. Each node has a weighted connection to several other linked nodes in adjacent layers. Single node take input received from linked nodes and use the weights of the connected nodes together with easy function for computation of output values. Neural networks can be created for supervised and/or unsupervised learning. The user specifies the number of hidden layers along with the number of nodes within a specific hidden layer. The output layer of the neural network may contain one or several nodes depending upon the application. Recently, neural network researchers have several associated methods from statistics and numerical analysis into their Networks. From the Given cases, nonlinear mapping relations from the input space to output space. Neural networks can learn and summarizes the internal assumptions of data even without knowledge of the potential data principles in advance. Statistical methods are sometime unusual in the practice research even though the common advantages of the neural networks in application of credit card fraud detection.

B.Data Mining

Data mining is popularly used to combat frauds because of its effectiveness. It is a well-defined procedure that takes data as input and produces models or patterns as output. Neural network, a data mining technique was used in this study. The design of the neural network (NN) architecture for the credit card detection system was based on unsupervised method, which was applied to the transactions data to generate four clusters of low, high, risky and high-risk clusters. The self-organizing map neural network (SOMNN) technique was used for solving the problem of carrying out optimal classification of each transaction into its associated group, since a prior output is unknown. The receiver-operating curve (ROC) for credit card fraud (CCF) detection watch detected over 95% of fraud cases without causing false alarms unlike other statistical models and the two-stage clusters. This shows that the performance of CCF detection watch is in agreement with other detection software, but performs better.

C.Clustering techniques

Two clustering techniques have been suggested for behavioral fraud by Bolton & Hand(2002). Peer group analysis is a system that allows identifying accounts which are behaving differently from others at one moment in time whereas previously, they were behaving the same. These certain accounts are then flagged as suspicious. Then fraud analysts have been used to uncover those cases. Hypothesis behind peer group analysis is that if accounts that were behaving the same for a certain period of time and then one account, still behaving significantly differently, then this account has to be notified.

D.Hidden Markov Model

Hidden Markov models (HMMs) are a formal foundation for making probabilistic models of linear sequence 'labeling' problems. They provide a conceptual toolkit for building complex models just by drawing an intuitive picture. They are at the heart of a diverse range of programs, including genefinding, profile searches, multiple sequence alignment and regulatory site identification. HMMs are the Legos of computational sequence analysis.In this section, it is shown that system of credit card fraud detection based on Hidden Markov Model, which does not require fraud signatures and still it is capable to detect frauds just by bearing in mind a cardholder's spending habit. The particulars of purchased items in single transactions are generally unknown 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.[1] The implementation techniques of Hidden Markov Model in order to detect fraud transaction through creditcards, 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, shipping address, and billing address and so on. The probabilities of initial set have chosen based on the spending behavioral profile of card holder 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.

IV. CONCLUSION

Credit card fraudulent detection which is done using HMM (Hidden Markov Model).This technique is used to detect various suspicious activities on credit card.It maintains a database,where past records of transactions are saved and any unusual transaction if carried out, which differs too much from the previous records, it tracks it.Let the user know by sending the details of the transaction on his mobile and hence prevent fraud.

V.FUTURE SCOPE

After evaluation of well-known Hidden Markov Model it is clearly shown the various methods which can detect the Fraud efficiently and provide accurate secuirity. Speed of the software can be enhanced by implementation of algorithms of less complexity.Inter mail server can be implemented using the same concept. Proper security provisions are made from malicious threats and hacking tools so that user account cannot be harmed intentionally or non-intentionally from frauds. Proper hierarchy of the users is maintained as per authority to access the data and use the services provided by the authority. Track all the necessary details during transaction process.

REFERENCES

[1] SHAILESH S. DHOK,Credit Card Fraud Detection Using Hidden Markov Model ISSN: 2231-2307, Volume-2, Issue-1, March 2012

[2] Ghosh, S., and Reilly, D.L., 1994. Credit Card Fraud Detection with a Neural-Network, 27th Hawaii International l Conference on Information Systems, vol. 3 (2003), pp. 621- 630.

[3] Syeda, M., Zhang, Y. Q., and Pan, Y., 2002 Parallel Granular Networks for Fast Credit Card Fraud Detection, Proceedings of IEEE International Conference on Fuzzy Systems, pp. 572-577 (2002).

[4] Stolfo, S. J., Fan, D. W., Lee, W., Prodromidis, A., and Chan, P. K., 2000. Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project, Proceedings of DARPA Information Survivability Conference and Exposition, vol. 2 (2000), pp. 130-144.

[5] Aleskerov, E., Freisleben, B., and Rao, B., 1997. CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection, Proceedings of IEEE/IAFE: Computational Intelligence for Financial Eng. (1997), pp. 220-226

[6] M.J. Kim and T.S. Kim, "A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection," Proc. Int'l Conf. Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002.

[7] W. Fan, A.L. Prodromidis, and S.J. Stolfo, "Distributed Data Mining in Credit Card Fraud Detection," IEEE Intelligent Systems, vol. 14, no. 6, pp. 67-74, 1999.

[8] R. Brause, T. Langsdorf, and M. Hepp, "Neural Data Mining for Credit Card Fraud Detection," Proc. IEEE Int'l Conf. Tools with Artificial Intelligence, pp. 103-106, 1999.