International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 25 Issue 5 – APRIL 2018 (SPECIAL ISSUE).

CREDIT CARD FRAUD DETECTION BASED ON THE TRANSACTION BY USING HIDDEN MARKOV MODEL AND PHP SOFTWARE

Antara Dey[#1] and R. Kavitha sudha[*2]

[#1] *M.Tech, Department of Embedded System and Technology, SRM Institute Of Science and Technology, Chennai, India*

[* 2]*Assistant professor of Embedded System and Technology, SRM Institute Of Science and Technology, Chennai, India*

Abstract- **Due to increase and growth of Electronic commerce, use of credit card is dramatically increased and parallely credit card fraud also increased explosively. Credit card base purchases are of two types, Those are :- i) Physical card base purchase, ii) Virtual card base purchase. For first type of purchase card holder contains a card for making a payment. In this type of purchase the fraudulent transactions can be done only if the attacker was able to steal the card from cardholder and the cardholder does not notice the loss of credit card. For the second type of purchase, only some important information of a card (card number, expiry date, secure code) is required. This can be happen due to not awareness of genuine card holder that someone else has seen or stolen all details of that card information. To detection of fraud activity recently we are using Hidden Markov Model (HMM). If an incoming credit card transaction is not accepted by the HMM, it is consider to be fraudulent. This paper presents a survey of various techniques used in credit card fraud detection mechanism.**

Keywords:**Hidden Markov Model, Fraud transaction, Credit card**

I INTRODUCTION

A large number of business, purchasing goods and services, even street vendors, these are now accepting cashless payments so that using of credit card is very increase and for offline transaction use of physical card and for online transaction we are using the virtual card. Credit card is easy to carry and easy to payments while on the move and for online purchase also it's easy to use butfraud activity of credit card is termed as an unauthenticated use of the system or we can call it as criminal activity. To detecting this kind of fraud activity have to analyse the spending patterns for every card and to figure out any inconsistency with respect to the "usual" spending patterns. For that implementation of efficient fraud detection systems are become imperative for all credit card issuing organization. Many modern techniques based on

Artificial Intelligence, Data mining, Machine learning, Generic programming etc., are evolved to detect credit card fraudulent transaction.

II EXPLANATIONS OF FRAUD TYPES

For financial transactions, the payment industry is innovating many technologies for secure environment. In existence there are many security advances like temper-evident, signature panel, EMV chip etc. has now become an industrial standards.

Fraud associated with credit card transaction:-

- Lost or stolen cards: It is commonone and due to irresponsible or unawareness of cardholder this type of fraud can happen.
- Account takeover: if a cardholder gives personal information (such as full name, address etc.) to a fraudster, who then contacts the cardholder's bank and can report lost card and ask to change personal information
- Counterfeit cards:if a card is "cloned" from another and then that one is using for purchase then this type of fraud can happen.
- Fraudulent application: if a fraudster uses another person's name and information to apply for and obtain a credit card.

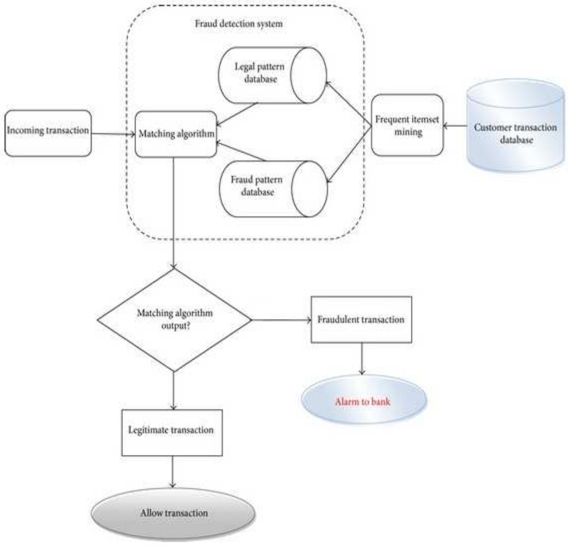
- Collusive merchants:if merchant employees work with fraudsters to defraud banks.

Staying alert about protecting personal information is greatly reduce risk of theft or fraud, an important and good step in today’s digital world. To protect from fraud transaction cardholder must not be disclose any information.

III HIDDEN MARKOV MODEL

It is a statistical markov model in which the system being model and is assume to be a Markov process with unobserve(i.e. hidden) states.It can be represent by the simple dynamic Bayesian network. In Hidden Markov Model output is depending on the state but states are not visible directly. Output tokens are depends upon the probability distribution of each states. Sequence of output tokens are generating by an Hidden Markov Model and it’s giving an idea about the sequence of states.

Hidden Markov Model is perfect for addressing detection of the fraud transaction. All transaction is submitted to the fraud detection system for verification purpose and to verify the transaction is genuine or not, card details such as credit card number, CVV number, card type, expiry date is required. The implementations techniques of this model is to detecting fraud transaction through credit cards, it’s creating clusters of training set and identify the spending spending profile of cardholder. Fraud detection system is only concentrate on the amount of item purchased and use for further processing, it’s not known the number of items, types of purchased. It stores data of different amount of transactions in form of clusters depending on transaction amount which is either high, low or medium ranges. It’s trying to find out any variance in the transaction base on the spending natural profile of the cardholder, shipping address, billing address and so on. If the fraud detection system makes sure that the transaction to be fraudulent, immediately it raises an alarm, and the particular bank declines the transaction. The security information module is stores all information into database for the security purpose. For that if the cardholder lost the card then the security information module form arises to accept the security information. On that security form security questions like account number, date of birth, nickname and other personal question and answer is present and user has to answer it correctly to move to the transaction section. Cardholder starts a credit card transaction processing by giving the credit card number, card type with expiry date and it’s storing into database. The details are received as network data in the database only if an accurate individual recognition code is used with the communication. Then only the cardholder or other authoritative can make transaction but if the transaction is pre-authorized, the vendor does not need to see or transmit an accurate individual recognition code.



Flowchart of HMM module for Credit card fraudulent detection

IV DESCRIPTION OF MODEL

If we check the existing models, the bank is verifying credit card information, CVV number, date of expiry etc. and those information are available on the card and easy for fraud transaction so recently bank is also asking to register credit card for online secure password. In Hidden Markov Model, after feeding details of card at merchant site, then it’s transfer to a secure gateway which is established at bank’s own server. HMM is helping to verify fraudulent of transaction which is going to happen and it’s having two modules:

i) Online Shopping: Now a days for online shopping many steps are presents, first is to login into a particular site from where goods and services can purchase and then choose any item and the next step is to go to payment mode where information or details of credit card is required. And after filling all those information that page will be directed to proposed fraud detection system which will be installed at merchant site or bank’s server.

ii) Fraud detection System: information details about credit card (like credit card number, CVV number, expiry date etc.) must be checked by the fraud detection system. If user entered correctly those details then system will ask Personal Identity Number (PIN) and that time also fraud checking activity activate on that system. The verification of all data is checking before loading the first page and before completing the ten transactions system can ask all details for each transaction, after completing ten transaction system will store the details into database and after if any change is showing for next transaction system again will ask all details or that particular transaction will be marked as fraudulent transaction. By using this type of observation system determine users spending profile and if the transaction may be concluded as fraudulent then user must enter security information (like account number, date of birth etc.) which are provide at the time of registration.

V PHP SOFTWARE

PHP is a server side scripting language designed for web development but it is used as a general purpose programming language. It is called as hypertext pre-processor. PHP code is joins into HTML code.

For credit card fraud detection method PHP module easily implement.

Features of PHP module:

- Credit card issuing bank validation
- Fraud analysis and scoring
- Email address validation
- Mobile app notification of fraud orders
- Blacklist validation
- Email notification of fraud orders
- IP address location

By using PHP software the credit card fraud detection features makes use of the behaviour and location of the user to check for unusual patterns. These patterns include user characteristics such as user spending patterns as well as user geographic locations to verify user’s identity. If any unusual pattern is given by user then system is rechecking all data. For that if any unusual patterns are given by user the system can ask to that user to login again or even block the user for more than three invalid attempts.

VI CONCLUSION

Here we discuss an application of HMM and using of PHP software in credit card fraud detection. Different steps of transaction are present in this model and software for security purpose. For HMM process we found that there are different range is present for transaction amount where types of purchasing items is considering the states of the HMM and using PHP software we can store data into database for bank details purpose and email connection to get alert while fraudulent transaction is going to happen. HMM system is scalable for handling large volumes of transaction. Using HMM and PHP software we can understand and getting alert the transaction is fraudulent or not.

VII REFERENCES

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

[2]. 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).

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

[4]. 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.

[5]. M.J. Kim and T.S. Kim, “A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection,” Proc. Int’1 Conf. Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002.

[6]. 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.

[7]. 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.

[8]. C. Chiu and C. Tsai, “A Web Services-based collaborative scheme for Credit Card Fraud Detection,” Proc. IEEE Int’l Conf. e-technology, e-commerce and e Service, pp.177-181, 2004.

[9]. C. Phua, V. Lee, K.Smith, and R. Gayler, “A Comprehensive Survey of Data Mining-Based Fraud Detection Research,” http://www.bsys.monash.edu.au/people/cphua/.Mar. 2007.

[10]. S. Stolfo and A.L. Prodromidis, “Agent-Based Distributed Learning Applied to Fraud Detection,” Technical Report CUCS-014-99, Columbia Univ., 1999.

[11]. C. Phua, D. Alahakoon, and V. Lee, “Minority Report in Fraud Detection: Classification of Skewed Data,” ACM SIGKDD Explorations Newsletter, vol. 6, no. 1, pp. 50-59, 2004.

[12].V. Vatsa, S. Sural, and A.K. Majumdar, “A Game-theoretic Approach to Credit Card Fraud Detection,” Proc. IEEE Int’l Conf. Information Systems Security, pp. 263-276, 2005.

[13]. D. Ourston, S. Matzner, W. Stump, and B. Hopkins, “Applications of Hidden Markov Models to Detecting Multistage Network Attacks,” Proc. 36th Ann. Hawaii Ini’l Conf. System Sciences, vol. 9, pp. 334-344, 2003.