International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

"Hidden Markov Model for Online Credit Card Transaction Fraud Detection"

Miss. Sarita M. Samatkar; Miss. Saba Kausar S. Ahmed & Miss. Lalita M. Nagpure

Miss. Sarita M. Samatkar: Computer Science & Engineering.
Miss. Saba Kausar S. Ahmed: Computer Science & Engineering.
Miss. Lalita M. Nagpure: Computer Science & Engineering.

1. Abstract:

Now a days,Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card as a fraudulent source of funds in a transaction. The most accept mode is credit card for both online and offline in today's world. It provide cashless shopping at every shop in all countries. So as credit card is becoming most popular mode for online financial transactions, at the same time fraud associated with it are also rising. In this paper HMM(Hidden Markov Model) is used to model sequence of operation in credit card transaction processing. HMM does not required fraud signatures it is initially trained with the normal behavior of a cardholder. If an incoming Online card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, we will attempt to guarantee that fraud transactions are rejected.At the same time, we will attempt to guarantee that fraud transactions are rejected.

2. Introduction:

Online-card-based purchases can be categorized into two types: 1) physical card and 2) virtual card. In a physical-card based purchase, the cardholder present his card physically to a merchant for making a payment.In this kind of purchase to carry out fraudulent transactions, an attacker has to steal the card. If the cardholder not realizes the loss of card, it can lead to a substantial financial loss to the Issuing card company. In a virtual-card based purchase, only some important data about a card (card number, expiration date, secure code) is required to make the transaction. Such type of purchases are normally done on the Internet or over the telephone. To commit fraud in such kind of purchases, a fraudulent simply needs to know the card details. Most of the time, the genuine cardholder is unaware about someone has stolen his card information. The only way to detect, fraud is to analyze the spending patterns on every card and to check out any inconsistency with respect to the "usual" spending patterns. Fraud detection based on analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful Online card frauds. Since users tend to exhibit specific behaviorist profiles, every cardholder can be represented by set of patterns

containing data 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.

3.Existing System:

In case of the existing system the fraud is detected after the fraud is done that is, after the complaint of the card holder fraud is detected. And so the card holder faced a lot of trouble before the investigation finish. And all the transaction is maintained in a log, we need to maintain a huge data. And also now a days many online purchases are made so we don't know the person how is using the card online, we just capture the IP address for verification purpose. So there need help from the cyber crime to investigate the fraud. To avoid the entire disadvantage we propose the system to detect the fraud in a best and easy way.

4.Technology Used:

In proposed system, we present a Hidden Markov Model (HMM) that does not require fraud signatures and is able to detect frauds by considering a cardholder's spending habit. The details of items purchased in Individual transactions are usually unknown for any Fraud Detection System (FDS) running at the bank that issues Credit/Debit cards to cardholder. Hence, we feel that HMM is an ideal choice for addressing this problem. Another important advantage of the Hidden Markov Model approach is a drastic reduction in the number of False Positives transactions identified as malicious by FDS although they are actually genuine. An FDS runs at a card issuing bank. Each incoming transaction is submitted to the FDS for verification. Fraud Detection System receives the card details and the value of purchase to verify, If the transaction is genuine or not. The types of goods that are bought in that transaction is unknown to FDS. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address and billing address, etc. If FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.

5.Advantages:

1.The detection of the fraud use of the card is found much faster that the existing system.
2.The transaction which is maintained in a log will also be a proof for the bank for the transaction made.
3.We can find the most accurate detection using this technique.
4.this reduce the tedious work of an employee in the bank

6. Conclusion:

1. We will have proposed an application of HMM in credit card fraud detection.
2. The different steps in credit card transaction method are represented as the underlying stochastic process of an HMM.
3. We will have used the ranges of transaction amount as the observation sign, whereas the types of item have been considered to be states of the HMM.
4. We will have suggested a process for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation sign and initial estimate of the model parameters.

5. It has also been explained how the HMM can find whether an incoming transaction is fraudulent or not.

7. Reference:

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] C. Phua, V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-Based Fraud Detection Research, Mar. 2007.