ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Survey on Credit Card Fraud Detection Using Hidden Markov Model

Bilonikar Priya[1], Deokar Malvika[2], Puranik Shweta[3], Sonwane Nivedita[4], Prof.B.G.Dhake[5]

Student, CSE Department, Savitribai Phule Womens Engineering College, Aurangabad, India[1,2,3,4]

Assistant Professor, CSE Department, Savitribai Phule Womens Engineering College, Aurangabad, India[5]

Abstract: In todays day to day life people mostly make use of online transactions for various banking transactions, shopping, etc. for that they make use of mostly internet banking that we called as E-commerce. As online Transactions are increasing so the frauds associated with it is also increasing.[14]In this paper we explained about how fraud is detected using Hidden Markov Model also care has been Taken to prevent genuine transaction should not be rejected by making use of one time password which is generated by server and sent to personal mobile of customer. Hidden Markov Model is the statistical tools for engineer and scientists to solve various problems.

Keywords: Internet Banking, Hidden Markov model, Probability, fraud Detection, Transaction.

I. INTRODUCTION

Now a day the usage of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising.

In day to day life credit card used for purchasing good and services by the help of virtual card for online transaction or physical card for offline transaction . In physical transaction, credit cards will insert into payment machine at merchant shop to purchase goods. Tracing fraudulent transactions in this mode may not be possible because the attacker already steal the credit card. The credit card may go in financial loss if loss of credit card is not realized by credit card holder. In online payment mode, attackers need only little information for doing fraudulent transaction (secure code, card number, expiration date etc.).

A. Hidden Markov Model

A Hidden Markov Model is a finite set of states each state is linked with a probability distribution. Transitions among these states are governed by a set of probabilities called transition probabilities. In a particular state a possible outcome or observation can be generated which is associated symbol of observation of probability distribution. It is only the outcome, not the state that is visible to an external observer and therefore states are ``hidden" to the outside; hence the name Hidden Markov Model. Hence, Hidden Markov Model is a perfect solution for addressing detection of fraud transaction through credit card. One more important benefit of the HMM-based approach is an extreme decrease in the number of False Positives transactions recognized as malicious by a fraud detection system even though they are really genuine.

To access internet banking, the customer would go to the financial instituation's website, And enter the internet banking facility using the customer number and password.[14] Some Financial institutions have set up additional security steps for access, but there is no consistency to the approach adopted. Credit card fraud cases are increasing every year. In 2008, number of fraudulent through credit card had increased by 30% because of various ambiguities in issuing and managing credit cards.

II. LITERATURE REVIEW

Credit card fraud detection has drawn a lot of research interest and a number of techniques, with special emphasis on neural networks, data mining and distributed data mining have been suggested.

Ghosh and Reilly [1] have proposed credit card fraud detection with a neural network. They have built a detection system, which is trained on a large sample of labeled credit card account transactions. These transaction contain example fraud cases due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud, and nonreceived issue (NRI) fraud. Recently, Syeda et al. [2] have used parallel granular neural networks (PGNNs) for improving the speed of data mining and knowledge discovery process in credit card fraud detection.

A complete system has been implemented for this purpose. Stolfo et al. [3] suggest a credit card fraud detection system (FDS) using meta learning techniques to learn models of fraudulent credit card transactions.

Meta learning is a general strategy that provides a means for combining and integrating a number of separately built classifiers or models. A meta classifier is thus trained on the correlation of the predictions of the base classifiers. The same group has also worked on a cost-based model for fraud and intrusion detection. They use Java agents for Meta learning (JAM), which is a distributed data mining system for credit card fraud detection A number of important performance metrics like True Positive—False Positive (TP-FP) spread and accuracy have been defined by them. Alekerov et al. [4] present CARDWATCH, a database mining system used for credit card fraud detection. The system, based on a neural learning module, provides an interface to a variety of commercial databases.

Kim and Kim[5] have identified skewed distribution of data and mix of legitimate and fraudulent transactions as the two main reasons for the complexity of credit card

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

fraud detection. Based on this observation, they use fraud density of real transaction data as a confidence value and generate the weighted fraud score to reduce the number of misdetections.

Fan et al. [6] suggest the application of distributed data mining in credit card fraud detection. Brauset al. [7]have developed an approach that involves advanced data mining techniques and neural network algorithms to obtain high fraud coverage.

Chiu and Tsai [8] have proposed Web services and data mining techniques to establish a collaborative scheme for fraud detection in the banking industry. With this scheme, participating banks share knowledge about the fraud patterns in a heterogeneous and distributed environment. To establish a smooth channel of data exchange, Web services techniques such as XML,SOAP, and WSDL are used. Phuaetal. [9] have done an extensive survey of existing data-mining-based FDSs and published a comprehensive report.

Prodromidis and Stolfo [10] use an agent-based approach with distributed learning for detecting frauds in credit card transactions. It is based on artificial intelligence and combines inductive learning algorithms and metal earning methods for achieving higher accuracy. Phua et al. [11] suggest the use of meta classifier similar to in fraud detection problems. They consider naïve Bayesian, and Back Propagation neural networks as the base classifiers.
A metaclassifier is used to determine which classifier should be considered based on skewness of data.Although they do not directly use credit card fraud detection as the target application, their approach is quite generic.Vatsa et al. [12] have recently proposed a game-theoretic approach to credit card fraud detection.

III. WORKING OF SYSTEM

In our proposed system of credit card fraud detection we are providing the account user with two Ids. First is the login Id for simply login in and doing the basic credit card transactions. Second Id is provided to the user that is the Profile-Id and its password using which the user can securely update his profile or if the users card is stolen then for security an option is provided for blocking his own card immediately when the user get login. For that the user has to enter his existing account number. Then the account Number is First Verified If the user is a valid user. Then only he is able to get the blocking option after blocking his own card. In This project, to avoid the inconvenience and stress of the user we have provided a facility to do all the transactions of the user by providing a virtual card.

A virtual card will be assigned by the admin to the user in which the user will get the virtual card no and password from the admin. In this we are using the ONE TIME PASSWORD for security purpose. Another security provided in this while doing the transactions are by using HMM MODEL algorithm in which we detect the fraud by analyzing the spending behavior of a particular user. If the spending habit of the user is determined to be having some different spending habits or there is large amount of expenditure going on suddenly. Then we may call it as a fraudulent person and we will ask him for the higher security Question before the transaction proceeds .Thus the fraud is detected and the user is very secure for using the credit card with full security.

Thus in this we provide the user with a high security to carry out transactions without any burden on him and suppose if the card is been stolen the user will be able to carry out his day to day transactions without any disturbance in his day to day business. Thus avoiding any stress and leading to profit.

IV. USE OF HMM TO DETECT FRAUD

A. System Architecture

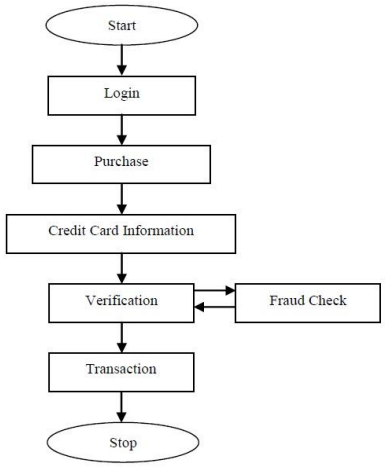

Fig 1: Architecture of Credit Card Fraud Detection

All the information about credit card (Like Credit card number, credit card CVV number, credit card Expiry month and year, name on credit card etc.) will be checked with credit card database. If User entered database is correct then it will ask Personal Identity number (PIN). After matching of Personal Identity number (PIN) with database and account balance of user's credit card is more than the purchase amount, the fraud checking module will be activated. The verification of all data will be checked before the first page load of credit card fraud detection system. 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, it concludes whether the transaction is real or fraud. If transaction may be concluded as fraudulent transaction then user must enter 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 transaction will not be fraudulent then it will direct to give permission for transaction. 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

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

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.

B. RFID Device

Fig 2: RFID Device

RFID stands for Radio Frequency Identification. RFID is one member in the family of Automatic Identification and Data Capture (AIDC) technologies and is a fast and reliable means of identifying objects. There are two main components: The Interrogator (RFID Reader) which transmits and receives the signal and the Transponder (tag) that is attached to the object. An RFID tag is composed of a miniscule microchip and antenna.

V. ADVANTAGES

1. The detection of the fraud use of the card is found much faster than the existing system.
2. The Transactions of the account holder never stopped As this system allows the user to use the virtual card Using the virtual ID and password, untill he gets the new card.
3. The user can easily block the card by himself when he finds that the card is being stollen.
4. In this system we have used the ONE TIME PASSWORD for the security to get the virtual ID and Password securely.
5. We can find the most accurate detection using this technique.
6. This reduces the tedious work of an employee in the bank.

VI. APPLICATIONS

1. Provide easy and well security to Online Shopping.
2. Detect Frauds and trace the Location from where the transaction has been made.

VII. CONCLUSION

In our paper we used an HMM in detection of credit card fraud. We modelled the sequence of transactions in credit card processing using an HMM. For swipping purpose we have used the RFID device to show the shopping transactions. We are detecting the fraud by firstly Observing the behaviour of the customer in which a High security questions page will be arrised. also if the card is stollen we have provided the user with the another profile ID and password and provided the ONE TIME PASSWORD for security purpose along with it we have provided the facility to the user for blocking the card immediately as soon as the card is stollen.

ACKNOWLEDGMENT

We would like to thank our guide Prof.B.G.Dhake, for their guidance and feedback during the course of the project. We would also like to thank our department for giving us the resources and the freedom to pursue this project

REFERENCES

[1] R. J. Bolton and D. J. Hand. Unsupervised profiling methods for fraud detection. In conference of Credit Scoring and Credit Connol VII, Edinburgh. UK, Sept 5-7,2001.
[2] Khyati Chaudhary, Jyoti Yadav, Bhawna Mallick, "A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications (0975 – 8887) Volume 45– No.1, May 2012
[3] K. C. Cox, S. G. Eick, G. J. Wills, and R. J. Brachman. Visual data mining: Recognizing telephone calling fraud.J Data Mining and Knowledge Discover, 1(2):22>231, 1997.
[4] Hollmn and Jaakko. Pmbabilistic Appmaches to Fraud Detecrion, Licentiate's ntesis. Helsinki University of Technology, Department of Computer Science and Engineering, 1999.
[5] X.D. Hoang, J. Hu, and P. Bertok, "A Multi-Layer Model for Anomaly Intrusion Detection Using Program Sequences of System Calls," Proc. 11th IEEE Int'l Conf. Networks, pp. 531-536, 2003.
[6] Masoumeh Zareapoor, Seeja.K.R, and M.Afshar. Alam, "Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria", International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, August 2012
[7] T. Lane, "Hidden Markov Models for Human/Computer Interface Modeling," Proc. Int'l Joint Conf. Artificial ntelligence, Workshop Learning about Users, pp. 35-44, 1999.
[8] Khyati Chaudhary, Jyoti Yadav, Bhawna Mallick, "A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications (0975 – 8887) Volume 45– No.1, May 2012.
[9] Hidden Markov Model by Jia Li. Department of Statistics "The PennsylvaniastateUniversity"http://www.stat.psu.edu/~jiali/course/stat597e/notes2/hmm.pdf.
[10] "A Revealing Introduction to Hidden Markov Models"by mark stamp.
[11] "Credit card Fraud Detection with a neural network" by Ghosh and Reilly.IEEE" Proceedings of the Twenty Seventh Annual Hawaii International Conference on System Sciences,1994.
[12] Offline Internet Banking Fraud Detection" by Vasilis Aggelis.
[13] "Security Analysis for Internet Banking Models By Osama Dandash, Phu Dung Le and Bala Srinivasan. Elighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing IEEE DOI.
[14] "Use of Hidden Markov Model as Internet BankingFraud Detection" By International Journal of Computer Application(0975-8887) Volume 45- No.21,May 2012
[15] "A Survey on Hidden Markov Model for Credit Card 3 Fraud Detection" By International Journal of Engineering and Advanced Technology(IJEAT) ISSN:2249-8958,Volume-1,Issue-3,February 2012.

BIOGRAPHIES

Miss.Priya P. Bilonikar is currently pursuing B.E.degree in Computer Engineering from Savitribai Phule Womens Engineering (University of marathwada). Intrested in ASP.NET, OS.

Miss.Malvika S.Deokar is currently pursuing B.E.degree in Computer Engineering from Savitribai Phule Womens Engineering (University of Marathwada). Intrested in ASP.NET, OS, DS, DBMS.

Miss.Shweta Puranik is currently pursuing B.E.degree in Computer Engineering from Savitribai Phule Womens Engineering (University of Marathwada). Intrested in ASP.NET, OS, DBMS.

Miss.Nivedita Sonwane is currently pursuing B.E.degree in Computer Engineering from Savitribai Phule Womens Engineering (University of Marathwada). Intrested in ASP.NET , OS, DS.

Prof.Bhavna G.Dhake is working as a Assistant Professor in Savitribai Phule Womens Engineering College. Intrested areas are Data Base, ASP.NET, Java.