DETECTION OF FRAUD IN ONLINE CREDIT-CARD TRANSACTIONS

Deepak Pawar[1], Swapnil Rabse[2], Sameer Paradkar[3], Naina Kaushik[4]
Student, Computer Department, Rajiv Gandhi Institute of Technology, Maharashtra, India
deepakpawar618@gmail.com

Abstract— **The main aim of project is to develop a system which identifies and detects fraud in online credit card transactions accurately. The system follows a multi-layered approach for security based on the amount of the transaction. We have used the probabilistic algorithm, an improvement on the Hidden Markov Model to detect frauds more efficiently. The algorithm calculates a threshold value based on the previous transactions and classifies them into 3 categories-low, medium and high. The current transaction is compared with the threshold value and on the basis of the calculated probability it is classified as fraud or not. The system also implements certain authentication mechanisms to detect the fraud in real time and block the transaction if the user is not found to be legitimate.**

Index terms- **Probabilistic algorithm, Credit card fraud, Hidden Markov Model, Data mining.**

I. INTRODUCTION

Today due to rapid growth in e-commerce online shopping or online transaction is grown day by day. The mode of payment is done by credit card. The credit card users are increasing day by day. It was reported that there are almost 430 million credit and debit card users across whole Europe. As the number of credit/debit card users increasing, the fraudulent users are also increasing.

There are two types of credit cards. 1] Physical card. 2] Virtual card. In the physical card [1,2 6], the user has to show the card while making payment. In this type, if fraudulent user wants to access his/her card then he just needs to steal that card. In virtual card, the fraudulent user needs to know the information about details information about credit card such as, CVV no, Secure code, Credit card number. Therefore the secure payment gateway is needed to identify the user and to verify that the user is legal or attacker. The most useful and appropriate technique used for fraud detection is Hidden Markov Model [5].

A. *Objectives*

- Creating an application to detect fraud Credit Cards.
- Implementing Hidden Markov model.
- Creating database containing all relevant information of Customer.
- Providing security to the customers at the time of transaction.
- Implementing firewall to restrict entry outside the Network

B. *Scope*

The system prevents fraudulent users from misusing the details of the credit-card of the genuine users for their personal gain. The spending habits of the credit-card owner is detect the fraud. As the fake user might not be aware of the spending habits of the owner, there will be an irregularity in the spending pattern, which the system will detect. The owner is immediately alerted about the attempted fraud and the transaction is blocked. Thus, the system protects legitimate users from financial loss.

The system helps in making electronic payment safer and more reliable. The principles in the proposed system can also be adopted and implemented in other electronic payment services such as online banking facility and payment gateways.

II. LITERATURE SURVEY

The review paper [3] gives the information about various types of fraud detection techniques. Which are resulting into restricting the fraudulent attacker from purchasing the products from legitimate user’s credit card. These research papers [1-2] gives the whole calculations of hidden markov model. This paper represent phases involved in the HMM algorithm as well as the architecture of system.

It is a very difficult task to identify the online fraud detection [4]. As no system can accurately/perfectly predict that the current transaction is fraudulent and done by an attacker. A good fraud detection system should contain the following properties:

1. Should detect the frauds quickly.
2. Should not consider legitimate user as fraud user.

III. HIDDEN MARKOV MODEL

A Hidden Markov Model works on finite set of states, distribution of probability is different for each state. A transition probability is obtained from probability of set of states. For a particular state, possible probabilities can be generated based on transition probability. The outcome which is not visible to external user and hence it is named as Hidden Markov Model (HMM). Hence, for detection of fraud in online transaction HMM is perfect solution. HMM classifies states probability into 3 categories such as: - 1) Low 2) Medium 3)

High. Because of this classification false positive transactions are decreased.

IV. EXISTING SYSTEM

In case of credit card fraud detection the existing system is detect the fraud after fraud has been happen. Existing system maintain the large amount of data when customer comes to know about inconsistency in transaction he/she made complaint and then fraud detection system start it working. It first tries to detect that fraud has actually occur after that it starts to track fraud location and so on. In case of existing system there is no confirmation of recovery of fraud and customers satisfaction.

V. PROPOSED SYSTEM

The aim of the proposed system is to develop a website which has capability to restrict and block the transaction performing by attacker from genuine user's credit card details. The system here is developed for the transactions higher than the customers current transaction limit.

As we seen the existing system detects the fraud after fraud has been occurred [1, 2] i.e. based on customers complained. The proposed system tries to detect fraudulent transaction before transaction succeed

1) In proposed system, while registration we take required information which is efficient to detect fraudulent user activity.

2) In proposed system we are using Hidden markov model (HMM) which works on transaction behavior of user. By Using HMM, after certain transactions we find one threshold value by using this threshold value we can compare current transaction with threshold value if transaction is quite different from user behavior then check whether it is genuine or fraud OTP (full form) and security questions are used.

3) HMM's working is quite good after certain transactions i.e. after 10 transactions .So HMM get failed when the transaction is users 1st or less than10 so to overcome this disadvantaged we take limit from user to protect first 10 transactions from fraudulent user.

4) To get security from hackers we are providing encryption at registration time for password this encryption is done by Secure Hash Algorithm (SHA) algorithm

A. Working:-

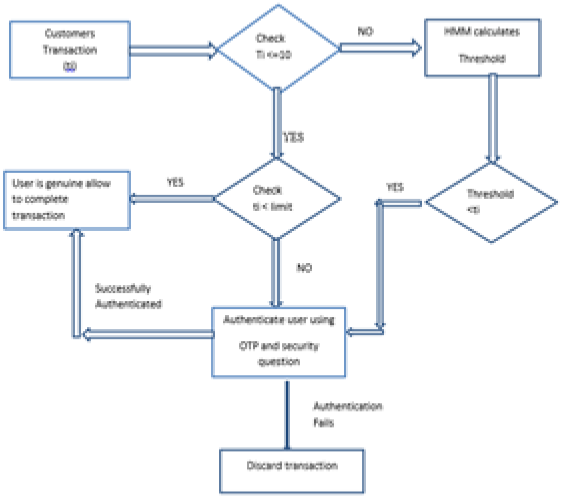

Fig 1. Working of Proposed System

1. Here t1, t2, t3 .... are set of transactions where t1 is individual transaction and c1, c2, c3.... are set of counters respective to each transaction.

2. For particular customer if he is performing his transaction then counter c will increase after successful transaction.

3. In Fraud detection phase while customer is performing his transactions the counter will be checked i.e. if. Ci <10 then customers limit will be checked if transaction and limit are nearby then customer will able to perform transactions by filling particular details. If Ci >10 then HMM comes into picture here threshold value generated by HMM will be checked and according to this value further transaction will be handled

VI. FUTURE WORK

Speed of the software can be enhanced by implementation of algorithms of less complexity.

VII. CONCLUSION

In these proposed system we analyzed and detect the fraud in online credit-card transactions in real time. Also the algorithm implements a multi-layered approach for security based on the amount of the transaction. It classifies the transactions according to the spending habits of the customer and calculates a threshold value which helps in detecting whether the current transaction is genuine or not.

VIII. ACKNOWLEDGMENT

We would like to take opportunity to thank to Prof. Naina Kaushik to provide necessary support and guidance to carry out the research work. We also value her eagerness and enthusiasm in encouraging us to develop our technical and creative ideas, which ultimately led to success of our project. Our special thanks to faculty members of Computer Engineering Department for their great support and kind co-operation to provide us with whatever we require for our project.

REFERENCES

[1] D. P. Deepti, M. K., Sunita, M. W. Vijay, J. A. Gokhale and S. H. Prasad, Computer Science and Network Security, vol. 10, no. 8, (2010).

[2] S. O. Falaki, B. K. Alese and W. O. Ismaila, Practical Mathematics and Computing, vol. 1, no. 2, **(2010).**

[3] S. Esakiraj and S. Chidambaram, "A predictive aproach for fraud detection using hidden markov model" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, January- 2013 C

[4] Suman nd Nutan **"**Review paper on credit card fraud detection", International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[5] V. Bhusari, and S. Patil, "Study of Hidden Markov Model in Credit Card Fraudulent Detection", International Journal of Computer Applications (0975 – 8887) Volume 20– No.5, April 2011

[6] P. Jayant, Vaishali and D. Sharma "Survey on Credit Card Fraud Detection Techniques" International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 3, March - 2014