ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Credit Card Fraud Detection System using HMM and Image Click Point Authentication

Vishwesh Satyanarayan Rathi, Prajakta Vilas Kanhaiye, Kajal Ratankumar Nankani, Deepali Naresh Nara

Students, Department of Computer Engineering, SSBT COET, Bambhori, Jalgaon, India

ABSTRACT: The Credit Card has become a popular mode of payment for online as well as offline purchases, as a result online fraud also increases. The credit card frauds are increasing day- to- day, along with that the multiple techniques are also developed for credit card fraud detection. The fraudsters are so talented and they generate new ways for committing fraudulent transactions on each day, which demands constant modernization for its detection techniques. Most of the techniques based on Artificial Intelligence, Machine Learning, Fuzzy Logic, Neural Network, Sequence Alignment, Decision Tree, Meta Learning, Genetic Programming, Hidden Markov Model. The proposed system gives the solution for identification of most likely image regions to users and the user has to click on region of image for creation of graphical authentication in the Image Click Point Authentication System (ICPA). An Image Click Point Authentication is an order of points, chosen by the user in an image, displayed on the screen. An image contains regions and the graphical authentication sequence string generated when the user clicks on these regions. The system analyses possible attacks and blocks particular account which is attack by fraud.

KEYWORDS: Artificial Intelligence; Machine Learning; Fuzzy Logic; Neural Network; Sequence Alignment ;Decision Tree; Meta Learning; Genetic Programming; Hidden Markov Model.

I. INTRODUCTION

The bank provides debit or credit card for online purchasing. The card based purchases are categorized into two types virtual card and physical card. In both the cases, if the card or card details are lost the defrauder can easily commit fraud transactions, which results in money loss of card holder. In online fund transfer user use the details such as login id, One Time Password (OTP) and password. If the details of the credit card are mistreated then it gives result as increase in fraud transaction [1]. The credit card fraud is a habitual term for fraudster. The purpose of fraudster is to obtain goods without paying or to obtain unapproved amount from an account.

It has been observed that many research indented to enhance the credit card fraud detection system and the Hidden Markov Model (HMM) is the best solution for fraud detection in credit card. But due to some limitations like inaccurate results, user behaviour based security, no secret authentication and no strong transaction checking, the goal of accurate credit card fraud detection is not achieved. The goal can be achieved by providing Image Click Point Authentication (ICPA) in proposed solution.

II. RELATED WORK

In [1] authors presented Decision Tree algorithm which is data mining induction technique that recursively divide a dataset of records using depth first greedy approach. A decision tree structure is made of root, internal nodes, leaf. The tree structure is used in sorting unknown data records. In this method, a credit card fraud detection using useful algorithm for Decision Tree Learning and focus is on the information growth based. This method estimates the best split of purity measures, entropy and information gain ratio to test the best classifier attribute. The author simply find out the fraudulent user through tracing fake mail and IP address. Customers are suspicious if the mail is fake and they traced all details about the sender through IP Address.

In [2] authors presented fraud detection using Neural Network is totally based on the human brain working principle. There is a fix pattern of credit card use, made by the way consumer uses a credit card. When credit card is being used by unauthorized user the Neural Network based fraud detection system check for the pattern used by the

DOI: 10.15680/IJIRCCE.2017. 0503168

fraudster and matches with the pattern of the valid card holder on which Neural network has been trained. If the pattern matches, then the Neural Network declare the authorize transaction.

In [3] authors presented a HMM is a double embedded stochastic process with two hierarchy levels. It is complicated stochastic processes as compared with traditional Markov Model. A Hidden Markov Model (HMM) has a finite set of states monitored by a set of transition probabilities. An observation or an output generated according to an associated probability distribution in particular state. It is only the output and not the state that is visible to an external observer. HMM uses cardholders spending behaviour to detect fraud. In implementation, there are three behaviours of cardholder are taken into consideration, High spending behaviour, Medium spending behaviour, Low spending behaviour. Different users have their various spending behaviour (high, medium, low). High spending behaviour of any user shows that cardholder spend high amount (H), medium spending behaviour of any user shows that user spend medium amount (M), low spending behaviour of any user shows that cardholder spend low amount (L).

III. Proposed algorithm

The architecture is a system that unifies its components or elements into a coherent and functional blocks. The architecture shows the structure of system. The architecture of credit card fraud detection system consist of two parts, viz., Administrator (Bank Part) and Card Holder (User Part).

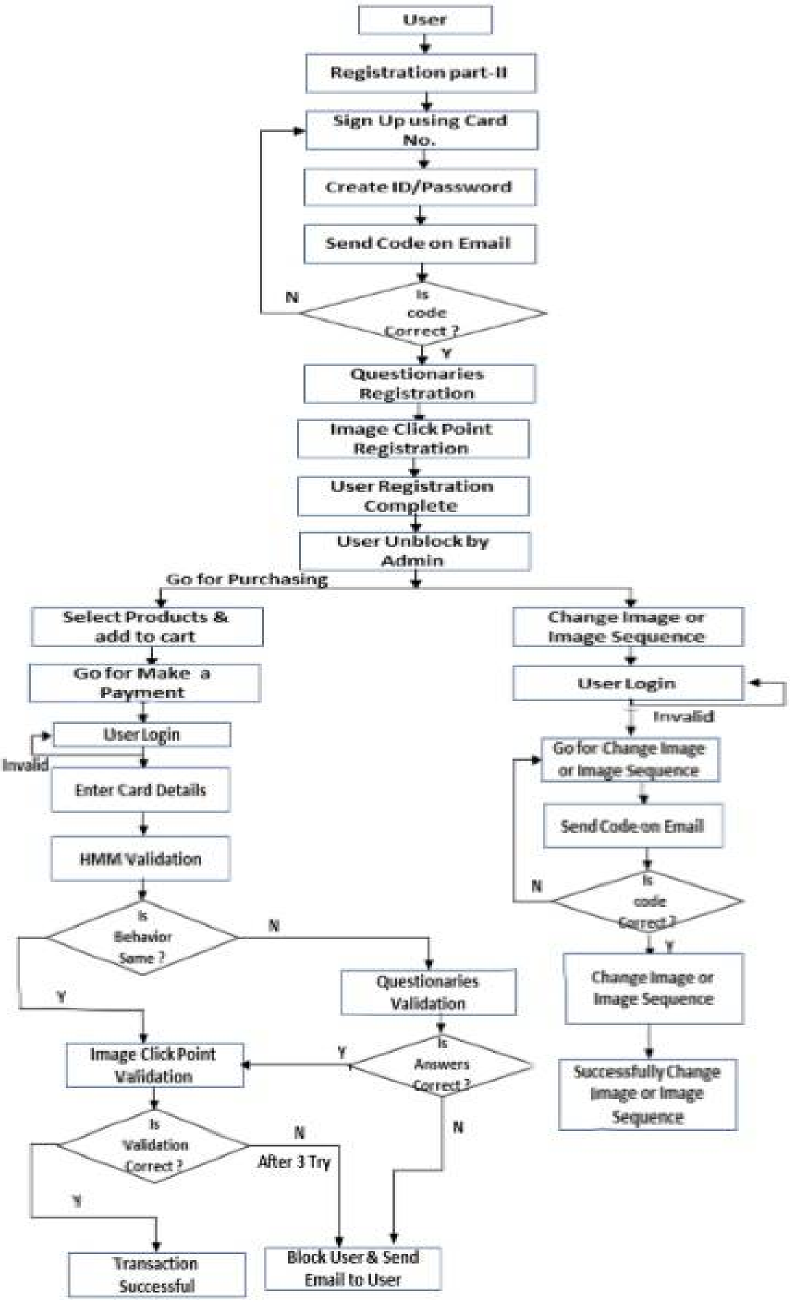
The administrator is responsible for registration of credit card holders or user with details [4]. This part consist of registration of user's credit card details, transaction details, user behavior, and locked status of user. The Admin accepts some basic details of user for registration part-I like, credit card number, name of user, address, e-mail id, mobile number, Pin code. While accepting credit card number, system checks if it is existing or not, if it is existing, system gives alert and not allowed for duplicate registration. That means single credit card registration at single time. Once credit card number is registered, same number is not allowed for registration by the system. Administrator also checks behavior of user along with all transaction of every user. User behavior shows the status of user. The status is define after validation of HMM. The HMM are used to identify the behavior of user and defines its status. The behavioral status are three parts, low, medium and high. The system displays blocked and unblocked status of all users. When a fraud is detected, the system immediately blocks respective user. Hence, user is not allowed to perform any transaction. On the other hand, administrator has a right to activate and deactivate the users.

The part of user is part of architecture in which user can complete remaining registration and purchase his required things. The architecture of credit card fraud detection system is shown in Fig. 1. The work of proposed system is described in this block. Hence, some blocks are related to user and are discussed below.

Card Holder should complete remaining registration in registration part-II. User completes registration process by entering credit card number. Once the user has entered this part, basic details are filled by the system which is already entered by administrator. User only needs to create user id and password. The system accepts user id and password, and sends a four digit code on registered email-id for more security purpose because email is more secure than mobile number. If four digit code is matched then the system identifies the user as authorized user then questionnaires are provided to the user. The user needs to fulfill all the questionnaires to confirm registration [4]. These questionnaires are occurred when the change in behavior is found by HMM. After questionnaires, system asks Image Click Point Authentication (ICPA), in which user need to select maximum four objects on an image and make a sequence. In this way, user completes the registration. At the end of registration, user has three authentication viz., user id and password, questionnaires and Image Click Point Authentication (ICPA). But, at this stage user is not able to shop because at initial stage every user is in block stage. Therefore administrator needs to grant the permission then and only then the user performs transaction.

While user performs transaction, Hidden Markov Model (HMM) works effectively. The system accepts transaction amount and HMM find spending profile by checking last transaction. Every incoming transaction is passed to the HMM for verification. The system receives the details of card and the value of purchase and goods to verify whether the transaction is genuine or not. The type of product that are bought in that transaction are not known to the system. It tries to find fraud in the transaction based on the spending profile of the card holder. If the system confirm the transaction to be fraud it raises an alarm and ask for next for next module. The next step of the proposed system is Image Click Point Authentication (ICPA) validation and questionnaires for providing better security

The Image Click Point Authentication (ICPA) is a graphical authentication method. The graphical authentication method consists of three to four click points sequences, which are chosen by user. In authentication process, the user has to click repeatedly on exactly the same point. As per studies on graphical attention and eye movements show that, most of the images contain a few portions that most humans focus on. When asked to create a graphical authentication a user would probably not click on all available pixels, but focus on some specific areas.



IV. PSEUDO CODE

```
Step 1: Require: Behaviour status
Step 2: Ensure: Sufficient Balance
            If $T_{val} > T_{behavior}$ then
            Ask questions
            End if
Step 3: If answers are valid then
            Allow authentication
            Else
            Reject transaction and block user
```

Algorithm 1 Image Click Point Algorithm

```
Require: Initialize i=1 for no. of points selection
  Ensure: HMM variable
             Begin
             If  i<5 then
                    Calculate X and Y value of click point
             If X and Y are pixel of First object then
                    Display object marked image
                    Value = object1
                    Sequence no. = 1
                     i = i+1
             else if X and Y are pixel of Second object then
                    Display object marked image
                    Value = object2
                    Sequence no. = 2
                     i = i+1
             else if X and Y are pixel of Third object then
                    Display object marked image
                    Value = object3
                    Sequence no. = 3
                    i = i+1
            else if X and Y are pixel of Third object then
                    Display object marked image
                    Value = object3
                    Sequence no. = 3
                    i = i+1
            else if X and Y are pixel of Fourth object then
                    Display object marked image
                    Value = object4
                    Sequence no. = 4
                    i = i+1
            else if X and Y are pixel of Fifth object then
                    Display object marked image
                    Value = object5
                    Sequence no. = 5
                    i = i+1
            else if X and Y are pixel of Sixth object then
                    Display object marked image
                   Value = object6
```

```
        Sequence no. = 6
        i = i+1
**else if** X and Y are pixel of Seventh object **then**
        Display object marked image
        Value = object7
        Sequence no. = 7
        i = i+1
**else**
        No. of objects selection is over
**end if**
End
```

V. SIMULATION RESULTS

Image Click Point Authentication (ICPA) increases the transaction security and block fraudulent transaction immediately before processing the payments. ICPA method provides maximum security. On every transaction, system is updated and take valid decisions as per user behaviour. According to observations, users are more secure and perform faithful transactions.

In existing system the fraud is detected only on the basis of change in behaviour of user. In this case, if valid user performs wrong transaction then change in behaviour occurs and user is blocked immediately. This problem is solved in proposed system by providing three level security to identify a valid user. The proposed system gives three attempts to the user for validation, and hence the proposed system is superior to existing system.

In the Table 1 'Transactions Status with Overall Observations'[4] shows the number of transaction per user with all statistical states, in which some observations like, how much number of times user entered in change in behaviour. In some cases, if upcoming transaction is differ from existing behaviour then user must face the questionnaires and Image Click Point Authentication. In the image click points if user cannot fallow the correct sequences then system gives three attempts, after three attempts user is blocked. 'False positive' parameter shows the unsuccessful transactions and 'True positive' shows successful transactions or user block status. By analyzing all transactions success rate of true positive transactions is much greater than existing systems.

Sr. No.	No. of Transaction	Change in Behaviour	No. of times questions asked	No. of times Image Click Points	True positive	False positive	Success rate in percentage
1.	10	2	2	15	8	2	80.00
2.	12	3	3	14	10	2	83.33
3.	11	2	2	15	11	0	100.00
4.	09	1	1	13	6	3	66.67
5.	10	3	3	20	8	2	80.00
6.	10	1	1	16	7	3	70.00
7.	14	2	2	20	12	2	85.71
8.	15	1	1	25	11	4	73.33
9.	13	1	1	23	12	1	92.31
10.	12	2	2	17	12	0	100.00

Now-a-days, HDFC gives similar kind of security in the form of image identification. But there is no any secret point and once image is watched by anyone then it is easy to identify that image. According to the survey, there is no such type of three level security. Many banking sectors use One Time Password (OTP) using mobile number for password verification. But problem is that the mobile number not in network, the messages may be diverted on another number by fraudulent. Hence proposed work uses email id for verification, system sends four digit OTP code on registered email id. In this way proposed solution is better than others.

VI. CONCLUSION AND FUTURE WORK

The credit card fraud detection system gives four level security by using Hidden Markov Model and Image Click Point Authentication. Proposed system solves drawbacks of existing system i.e. inaccurate results, user behaviour based security, no secret authentication and no strong transaction checking. The proposed system does not blocked a valid user and faithful transaction with authentication facility carried out through email id. The calculating performance of proposed system is handled by different users and created dataset. The user updated dataset is observed and the observations are defined on the basis of some parameters like number of users, number of transactions, change in behaviour and number of true or false transactions. According to observations, system provides 80 to 95 percent security for transactions. The maximum transactions becomes true transactions but only the drawback is, user is harassed due to more security levels but it is negligible for strong security. The system allows the user to change the click point sequences or to change the images for new sequences hence security also increases.

REFERENCES

1. R. Dhanpal and P. Gayathiri, “Credit card fraud detection using decision tree for tracing email and ip", International Journal of Computer Science Issues, Vol. 9, no. 2, 2012.
2. R. Patidar and L. Sharma, “Credit Card Fraud Detetion Using Neural Network”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-NCAI2011, June 2011.
3. A. Srivastava and A. Kundu, “Credit card fraud detection using hidden markov model", IEEE Transactions on Dependable and Secure Computing, Vol. 5, no. 1, 2008.
4. K. P. Adhiya and Dinesh L. Talekar, “Credit card fraud detection Using Hmm and Image Click Point Authentication”, International Journal of advanced studies in Computer Science and Engineering IJASCSE, Volume 4, Issue 3, 2015.
5. V. Bhusari and S. Patil, “Study of hidden markov model in credit card fraudulent detection", International Journal of Computer Applications, vol. 2, no. 5, 2011.
6. R. D. Patel and D. K. Singh, “Credit card fraud detection prevention of fraud using genetic algorithm", International Journal of Soft Computing and Engineering (IJSCE), vol. 2, no. 6, 2013.
7. K.RamaKalyani and D.UmaDevi, “Fraud detection of credit card payment system by genetic algorithm", International Journal of Scientific Engineering Research, vol. 3, no. 7, 2012.
8. S. Vats, S. K. Dubey, and N. K. Pandey, “A tool for effective detection of fraud in credit card system", International Journal of Communication Network Security, vol. 2, no. 1, 2013.
9. A. Singh and D. Narayan, “A survey on hidden markov model for credit card fraud detection, "International Journal of Engineering and Advanced Technology (IJEAT), vol. 1, no. 2, 2012.
10. ShendageSwapnil Sunil et al, “Cued Click Points: Graphical Password Authentication Technique for Security”, InternationalJournal of Computer Science and Information Technologies, Vol. 5 (2), 2014.
11. Gaurav Mhatre et al, “Credit Card Fraud Detection Using Hidden Markov Model”, International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2053-2055.
12. Nitin B. Khandare, “Credit Card Fraud Detection Using Hidden Markov Model”, International Journal of Advance Scientific Research and Engineering Trends, Volume 1, Issue 4, July 2016.

BIOGRAPHY

Vishwesh Satyanarayan Rathi, Prajakta Vilas Kanhaiye, Kajal Ratankumar Nankani, Deepali Naresh Nara are the Students of Computer Engineering Department, SSBT COET, North Maharashtra University, Bambhori - Jalgaon India. They all are the students from final year of Bachelor of Computer Engineering (BE) degree.