METHOD (ICPA) AND SYSTEM FOR DETECTING ONLINE FRAUD TRANSACTION USING HIDDEN MARKOV MODEL

Somnath A. Gade
Research Scholar, Department of CSE
SVCSHE, Alwar, India
E-mail-somnathgade.414@gmail.com

Sunil Gupta
Associate Professor, Department of CSE
SVCSHE, Alwar, India
E-mail-sunilgupta8764@gmail.com

Abstract
In this paper Image Click Point Authentication application is used on any online operation using Hidden Markov model. Credit card frauds are increasing day by day irrespective of the numerous techniques established for its discovery. Fraudsters are skillful that they prompt different methods for committing fraudulent transactions each day which demands constant innovation for its detection techniques as well. Many techniques based on Artificial Intelligence, Data mining, Fuzzy logic, Machine learning, Sequence Alignment, decision tree, neural network, logistic regression, naïve Bayesian, Bayesian network, meta learning, Genetic Programming etc., has evolved in detecting numerous credit card fraudulent Transactions. This paper attention on creating a password by using a sequence of four click-points on image contributes to password. User authentication is one of the most important procedures required to access secure and important data. Authentication of users is usually achieved through text-based passwords. Attackers through social E-commerce techniques easily obtain the text based password of a user. Today's world is Internet world. Now-a-day attraction of E-commerce is increasing tremendously. Using E-commerce people do their economical transaction online like online shopping etc. Most popular mode for online and offline payment is using credit card, use of credit card has radically increased. So as credit card is becoming very popular mode for online financial transactions, at the same time fraud related with it are also rising. In this paper Hidden Markov Model (HMM) is used to model the sequence of operation in credit card transaction processing.. An Image Click Point Authentication is a sequence of points, chosen by the user in an image that is displayed on the screen. An image contains regions and the graphical authentication sequence string is generated when the user clicks on these regions. The system analyses probable attacks and blocks particular account which is being attacked**.**

Keywords:- Image Click Points, (HMM), Credit Card, Online Fraud Detection Techniques, online shopping.

1 INTRODUCTION

The Internet has provided an ideal ground for fraudsters to commit credit card fraud in an easy way. The bank issues 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 fraudster 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, password and One Time Password (OTP). If the details of the credit card are misused then it gives result as increase in fraud transaction. The credit card fraud is a habitual term for fraudster. The purpose Fraudsters have recently begun to operate on a truly worldwide Understanding Credit Card Frauds level. With the expansion of trans-border or 'global' social, financial and partly-political places, the internet has become a New World market, catching consumers from most countries around the world. The most commonly used procedure in internet fraud are described below:

Site cloning:. Customers have no reason to trust they are not dealing with the company that they wish to purchase goods or services from because the pages that they are viewing are identical to those of the real site. The cloned or deceived site will receive these details and send the customer a receipt of the transaction via email just as the real company would. The customer suspects nothing, whilst the fraudsters have all the details they need to commit credit card fraud [3][4].

False merchant sites:. The site requests a customer's complete credit card details such as name and address in return for entree to the content of the site. Typically text passwords are string of letters and numbers, i.e. they are alphanumeric. even through text passwords should be both memorable and secure, in practice, most passwords are each one memorable but easy-to-guess or secure but difficult-to-remember Graphical passwords have been designed to make passwords creasing growth of credit card use on the internet has made database security lapses particularly costly. Today the most common user authentication scheme is the

alphanumeric password in computer systems [2]. Alphanumeric passwords are used widely; it's assured well known weakness is low memory ability of high information passwords. This weakness is not because of the authentication system itself but arise from the interaction between the users and the system. Since users usually cannot remember high information passwords they tends to select short or simple passwords that can be broken by dictionary attacks. Policies and mechanisms that force users to select high information passwords usually results in other unsafe practices, such as the passwords being written down and kept open. There are multiple techniques to improve the security of user authentication, e.g., token based authentication, biometrics, graphical passwords based on the simultaneous use of two or more authentication mechanisms [7].

1.1 **MOTIVATION**

The main motivation for graphical authentication is the possibility that people are better in identification images than artificial words Therefore if we think about above frauds and their impacts it is necessary to have some discovery systems. Some credit card fraud discovery systems have been developed by many researchers. The proposed work defines technique to avoid computational complexity and to provide more accurateness in fraud detection. The main motivation for graphical authentication is the possibility that persons are better in remembering images than artificial words. For example, the persons are recognized from thousands of aspects, this evidences was used to implement an authentication system. Another example is, a user could choice a sequence of points in an image as an authentication purpose which it leads to a vast number of probabilities, if the image is big and complex. Hence, the projected system provides high security to online transactions. The rest of paper is organized as follows. In Section II Related work, Section III discusses Methodology, Section IV discussed proposed methodology. In section V discuss performance evaluation and result analysis followed by a conclusion in Section VI.

II LITERATURE SURVEY

2. 1 IMPACT OF FRAUDS

A) Impact of Fraud on Cardholders: Many banks even have their own integrity that limits the consumer's liability to a greater extent. They also have a cardholder security plan in place that covers for most losses of the cardholder. The cardholder has to just report doubtful charges to the issuing bank, which in turn investigates the difficulty with the acquirer and dealers, and processes charge-back for the doubtful amount [12].

B) Impact of Fraud On dealers: dealers are the most affected party in a credit card fraud, principally more in the card-not-present transactions, as they have to be-leaved complete liability for losses due to fraud. Each and every time a legitimate cardholder doubtful a credit card charge, the card-issuing bank will direct a charge back to the dealers (through the acquirer), withdrawing the credit for the transaction. In case, the dealer does not have any physical evidence (e.g. delivery signature) available to challenge the cardholder's doubtful, it is almost impossible to reverse the charge back. Therefore, the merchant will have to completely absorb the experiences of the fraudulent transaction [12].

2.2 HMM TECHNIQUE

An HMM as a finite set of states governed by a set of transition probabilities. In a particular state, an out come or observation can be generated according to an associated probability distribution. It is only the outcome and not the state that is visible to an external viewer HMM uses cardholder's spending behavior to detect fraud. In our Implementation, three behavior of cardholder are taken into consideration. 1) Low spending behavior 2) Medium spending behavior 3) High spending behavior. Different cardholders has their different spending behavior (low, medium, high).Low spending behavior of any cardholder means cardholder spend low amount, medium spending behavior of any cardholder means cardholder spend medium amount, high spending behavior of any cardholder means cardholder spend high amount. These profiles are observation symbols, therefore M=3 [8].

Different cardholders have their different spending behavior (low, medium, high).Low spending behavior of any cardholder means cardholder spend low amount (L), medium spending behavior of any cardholder means cardholder spend medium amount (M), high spending behavior of any cardholder means cardholder spend high amount (H). These profiles are observation symbols [10].

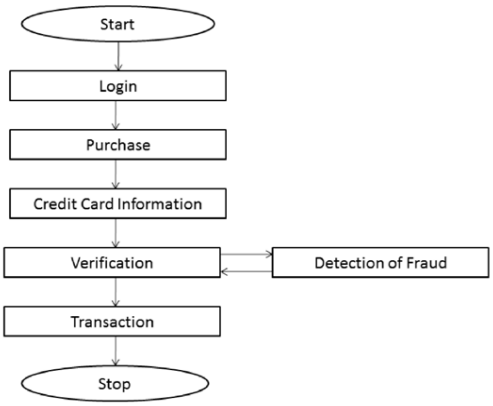

Figure 1: Flow of fraud detection system.

Author presented a HMM is a double embedded stochastic procedure with two hierarchy level. It is complicated stochastic processes as compared with conventional Markov Model. A Hidden Markov Model (HMM) has a finite set of

states observe by a set of transition probabilities. In a particular state, observation or an output generated according on the way to a connected probability distribution. It is only the output and not the state that is visible to an external observer. HMM uses cardholders spending behavior to detect fraud [10]. In execution, there are three behaviors of cardholder are taken into consideration, Low spending behavior, Medium spending behavior, High spending behavior. special users have their various spending behavior (low, medium, high). Low expenses behavior of any user shows that cardholder spend low amount (L), medium spending behavior of any user shows that user spend medium amount (M), high spending behavior of any user shows that cardholder spend high amount (H). Three clusters are formed using clustering algorithm and clusters represent observation symbols. The clustering probabilities are calculated for each cluster, which is percentage of number of transactions in every cluster then calculate fraudulent transactions [11]. In utmost cases, valid user is measured as fraudulent.

2.3 BACKGROUND

Alphanumeric passwords are the popular user verification method, but security and usability problems. Substitutes such as biometric systems and symbols have their own drawbacks. Graphical passwords proposal another substitute, and are the focus of this paper.

Image Click-point based graphical passwords: Graphical password systems are a variety of knowledge-based authentication that try to leverage the human remembrance for graphical information. A complete review of graphical passwords is available elsewhere. Of attention in this are cued-recall Image click-point graphical passwords . In such systems, users identify and target previously selected locations within one or more images. The images act as memory to support recall.

III METHODOLOGY

The existing system consist some drawbacks and proposed solution overcome this drawbacks by using ICPA (Image Click Point Authentication) technique. An Image Click Point Authentication is a sequence of points, chosen by the user in an image that is displayed on the screen. An image contains regions and the graphical authentication sequence string is generated when the user clicks on these regions. The system analyses possible attacks and blocks particular account which is being attacked. In proposed system, the need of bank authorization to create user, register credit card etc. Hence these assumptions are considered in proposed system. Along with banking side, assume online purchasing and payment delivery. The facts are assumed (1) User register in bank (2) Online purchasing.

3.1 ARCHITECTURE

The architecture shows the structure of system. The architecture of online fraud detection system is shown in Figure 2 The Architecture Consist of two parts: 1) Administrator (Bank Part), 2) User Part.

Administrator (Bank Part): The administrator is responsible for register credit card holders or user with details. This part consists of registration of user's credit card, transaction details, user behavior, and blocked status of user. Fig.2 shows administrator side structure. Administrator side consists of some functional block. 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 register 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 transactions of every user. Transactions are displayed with line graph. For every user, generate separate line graph on the basis of existing transaction. User behavior shows the status of user. The status is define after validation of HMM. The behavioral status are three parts Low, Medium and High. The system displays blocked and unblocked status of all user. When a fraud is detected, the system immediately block respective users, Hence users are not allowed to perform any transaction. On the other hand, administrator has a rights to activate and deactivate the users.

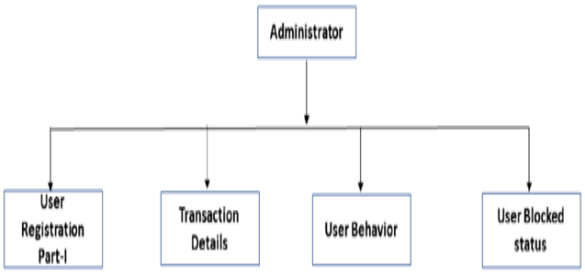

Figure 2: Architecture of Proposed Method for Credit card Fraud Detection at Admin Part.

User Part The part of user in which user can complete remaining registration and purchase the mandatory. Once the user has entered in 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 send OTP code on registered email id for more security purpose because email id is than mobile number. If is matched then system identifies the user as authorized user then questionnaires are provided to the user. These questionnaires are arisen when the change in behavior is found by HMM. After questionnaires', system asks Image Click Point Authentication (**ICPA**), in which user needs to select maximum four objects on an image and make the sequence. In this way user completes the registration. At the

end of registration, user has three authentications. While user carrying out transaction, Hidden Markov Model (HMM) work effectively. The system receive transaction amount and HMM find outgoings profile by checking latest transactions. Every incoming transaction is pass to the HMM for verification. The system collects the card information and the value of purchase a goods to verify whether the transaction is genuine or not. The types of product that are bought in those transactions are not known to the system. It tries to find any fraud in the transaction based on the spending profile of the cardholder. If the system authorizes the transaction to be fraud, it raises an alarm, and asks for succeeding module. To check and map the credit card transaction processing operation in terms of Hidden Markov Model, first selects the observation symbols in model. The values obtaining x into M price ranges V1, v2,...,Vm, creating the observation symbols at the issuing bank. The price range for each symbol is configure based on the spending practice of individual cardholders. The price ranges determined dynamically by applying a clustering algorithm (K-means algorithm) on the values of each cardholder's transactions. Here use Vk, k=1, 2, 3. M to represent the observation symbol and resultant price range. Consider three transactional price ranges, namely, low (l), medium (m), and high (h). So set of observation symbols is, therefore, V= l, m, h making M = 3. For example, let l= (0 < x < 50000), m= (50000 < x <100000) and h= (100000 < x < 200000); where x be transaction value. If a cardholder performs a transaction of 59000, then the corresponding observation symbol is m. Spending profiles of user are determined at the end of the K-means clustering step which is shown in Equation 1. Let pi be the percentage of total number of transactions of the users that belong to clusters. Then, the spending profile (SP) of the user is determined as follows:

$$SP = MAX_i (P_i) \quad (1)$$

Where Pi: Percentage of number of transactions
SP: Cluster number to which most of the transactions
The sequence of transactions are deliver to HMM and find out change in user behavior. Let O1, O2, O3, OR, one such sequence of length R. before new transaction initial behavior are set. First provide the initial sequence to Hidden Markov Model and compute the probability is shown in Equation (2) and define a behavior. Let the probability α1 which can be written as follows:

$$\alpha_1 = P (O_1, O_2, O_3....O_R|\lambda) \quad (2)$$

For new transaction Let OR+1 be the new symbol generated by a new transaction at time t+1, with length R. so new sequence is O1, O2, O3, OR, OR+1. Let new probability α2 is in Equation (3).

$$\alpha_1 = P(O_1,O_2,O_3....O_{R+1}|\lambda) \quad (3)$$

Now, check the any change are occurs in users spending profile behavior. Let, α be a difference of α1 and α2.

$$\alpha = \alpha_1 - \alpha_2 \quad (4)$$

Equation (4) calculate clusters symbol and find out the maximum number of transactions in clusters. In this process new cluster is compare with existing clusters. If α>0, it means that the new sequence is accepted by the HMM, and it could be a fraud. The symbol α denote change in user behavior are occurs, that means it is fraudulent transaction or second think is that, the valid user try to performing variation in transaction. Hence can't say that, it is definitely fraud. The proposed work is minimize same cases and implement new extended system. The Proposed system is provide next step for better security. The next step is Image click point validation and questionnaires. The Image Click Points Authentication (ICPA) is a graphical authentication method. The graphical authentication method are consists of click points (3 to 4 click points) sequences, which is chosen by user. The image is displayed on the screen by the system. The displayed image is helping to the user, remember the click points. The click point pixel in an image is a candidate for a click points. In the authentication process, the user has to click again on the chosen points. Hence it is almost possible for human users 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 only focus on some specific areas.
In the ICPA method, user has to select maximum any four objects in given image. The selected objects shown as selected regions, the selected regions define the probability of mouse click position. This model is defined probable regions with their pixel values. The system is create graphical authentication by calculating click point regions. The selected regions are stored in database by its name with sequence number, the sequence number shows specific object name in sequentially. The object names are useful when user forgot the password. The user can retrieve forgot sequence by matching verification code, which is send on registered email id by the system. When user select any object in the image, the system give the sequence number 1, while selecting second object system gives sequence number 2 in this way user select different objects and sequence numbers are provided automatically by the system. The name of object selected as per selection of region and the object positions are detected using given equation.

$$d_{posx} = (Px_{event} - I_{left}) \quad (5)$$

$$d_{posy} = (Py_{event} - I_{top}) \quad (6)$$

Equation (5) is used to calculate X position of mouse click point and Equation (3.6) is used to calculate Y position of mouse click point. Now, d_{posx} and d_{posy} contain X and Y coordinate of current click point, there for this coordinate map with ICPA method and define sequence number with object name. This object name is stored as per sequences for future authentication. Hence, ICPA method detects the fraudulent transactions and give more and more security to card holder.

IV PROPOSED ALGORITHM

The proposed algorithm described the catching click points on image object. The Image Click Point Authentication (ICPA) module asks to card holder after HMM validation that means behavior of user is not changed. The HMM checks the behavior of user using existing transactions. If the card holder's found in change behavior then system asks questionnaires for confirmation and if answers are correct then system allows to Image Click Point Authentication (ICPA) module. Once user come an Image Click Point Authentication (ICPA) the system initialize counter to 1. The user has to select any four object in given image. Algorithm firstly find the click point locations and then check with existing model. Existing model consist of specific object regions. All object region map with pixel values and then define the object name. On every selection object gives sequence number. The sequence number automatically incremented by one for next object selection, every object selection gives object name. Finally all object names are appended one another one and make a string and the string is stored in database as an authentication string. This authentication string match with new string, which is generated at the time of every Image Click Point Authentication (ICPA) for particular user. If string are not matched, then authentication failed and user is block. A key advantage of ICPA is that attackers need to analyze different subsets of images for different users means that an attacker must somehow gather information about the specific subset assigned to the current user .Algorithm 1 is used for accept the click points in given image and make a string sequence of object name.

Algorithm 1 ICPA Algorithm
Require: Initialize i=1 for number. of points selection
Ensure: HMM validation begin
if i < 5 then
Calculate X and Y value of click point.....Equation 5 and 6
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 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 Object selection is over end if
end if end

The final validation are done using verify sequence string with newly sequence, Algorithm 1 is used for accept the click points in given image and create string sequence of object name. Finally string verify with database string.

V EXPERIMENTAL DETAILS AND RESULT ANALYSIS

Experimental result shows the efficiency of proposed system, in which consider the some number of transaction from dataset. At initial condition dataset are filled by some user's activity. Initially clusters are created as per transaction values and then behavior of users calculated. As per behavior, user profile is set. According to profile system handles the users and allows or blocks the users. In Table 1 'Number of Transactions' shows the total 15 transactions, cluster algorithm helps to create a cluster. According to transactions, system defines user behavior and user behaviors are calculated by Hidden Markov Model. Below figure Shows the clusters for given transactions, in which x axis shows the number of transaction and y axis shows transaction amount and bubble dots shows the clusters. According to transactions, system defines user behavior and user behavior are calculated by Hidden Markov Model.

Transaction No.	Transaction Amount
1	13300
2	1300
3	4700
4	24200
5	10000
6	13200
7	19000
8	4800
9	1300
10	128000
11	480000
12	16100
13	120000
14	150000
15	120000

TABLE 1: NUMBER OF TRANSCATIONS.

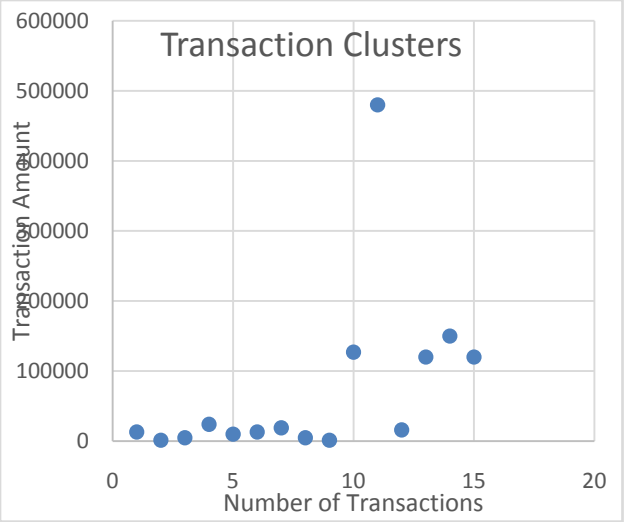

Figure 3: Data clustering.

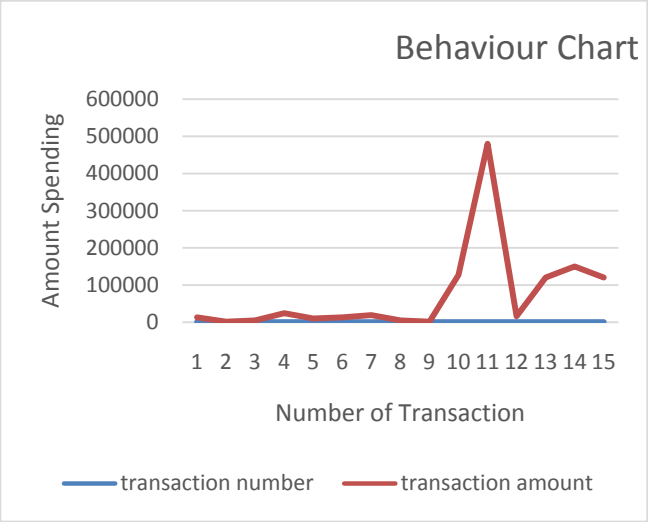

Figure 4: Behavioral result analyses from Table 1.

Figure 4: Shows that behavior of user lengthwise transactions which is shown in Table 4.6. If transaction amount is greater than 0 and smaller than 50000 then behavior consider as low, if transaction amount is greater than 50000 and smaller than 100000 then behavior is medium and if transaction amount is greater than 100000 then behavior is. Hence, finally behavior is defined for respective user.

Table 2. Transactions Status with Overall Observations shows the no's of transaction per user and completely statistical states, in which some observations like, how many times user entered in another behavior. In some cases, if next transaction is differ from older behavior then user must face the questionnaires and ICPA. If image sequence change then after unsuccessful three item user goes for block stage and confirmation message send to already registered email. 'True positive' shows the successive transactions and 'False positive' shows unsuccessful transactions or user block status. By examining all transactions success rate of true positive transactions is more than existing systems.

Sr. No.	No. of Transactions	Change In behaviour	No. of time Questions Ask	No. of times Image click points	True positive	False positive	success rate in percentage
1	10	2	2	15	7	3	70
2	13	3	3	14	11	2	84.615
3	11	2	2	15	11	0	100
4	10	1	1	13	7	3	70
5	9	3	3	20	8	1	88.888
6	12	1	1	16	9	3	75
7	13	2	2	20	11	2	84.615
8	14	1	1	25	11	3	78.57
9	15	1	1	23	12	3	80
10	14	2	2	17	13	1	92.851

Table 2: Transaction Status with Overall Observations.

I. DISCUSSION

Image click point Authentication (ICPA) increases the transaction security and block fraudulent transactions immediately before processing of payments. ICPA method provides maximum security. On every transaction, system is updated and take valid decision as per user's behavior. According to observations, users are more secure and performs faithful transactions. In existing system, the fraud is detected only on the basis of changing behavior of user. In this case, if valid user performs wrong transaction then change in behavior occurs and user is blocked immediately. This problem is solved in the proposed system by providing three level security to identify a valid user. The proposed system gives three attempts to the user to confirm the validity, and hence the proposed system is superior to existing system According to survey, there is no such type of three level security. Many banking sectors uses (OTP) using mobile number for final verification but problem is that if mobile numbers are out of coverage or switch off or someone stolen, the massages may be diverted on another number by fraudulent. Hence proposed work uses email id for verification, system sends OTP code on email id which is already registered. This way proposed solution is better.

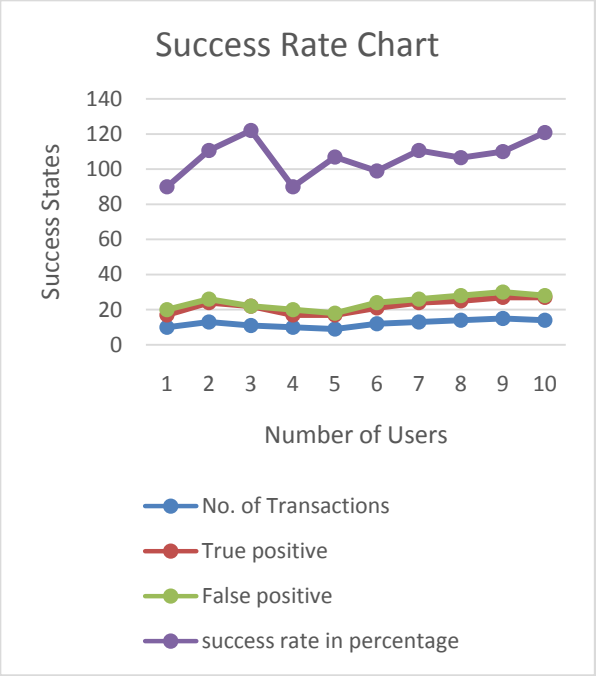

Figure 5: Transaction with success rate.

Figure 5show that graphical representation of success rate of proposed system, in given transactions near about 90 percent of transactions are successful. The rate true transactions are greater than false transaction. so that success rate is more than existing method.

VI CONCLUSION

The proposed ICPA scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images. The proposed system gives more level securities by using HMM and ICPA. Proposed system resolves drawbacks of existing system i.e. incorrectresults; user behaviors 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 define observations. The observations are defined on the basis of some parameters like number of users, number of transactions, change in behaviors and number of true or false transactions. According to observations, system provide 85 to 95 percent security for transactions. The maximum transactions become 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 sequences click hence security also increases. The proposed system consist of define images, user can not add new images, and cannot create new click point sequences. .The recognition of the fraud use of the card is found faster that the existing system. We can find the most accurate detection using this technique. In the future work, it is possible to new images and update it with different click point's sequences.

.

REFERENCES

[1] 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.

[2] V. K. Prasad, "Method and system for detecting fraud in credit card transaction", International Journal of Innovative Research in Computer and Communication Engineering, vol. 1, no. 5, 2013.

[3] 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.

[4] Y. Sahin and E. Duman, "Detecting credit card fraud by decision trees and support vector machines", Proceeding of the International Multi Conference of Engineers and Computer Scientist, vol. I, 2011.

[5] V. M. Rao and Y. P. Singh, "Proceeding of the international conference on artificial intelligence in computer science and ict", International Journal of Advanced Research in Computer and Communication Engineering Organized by WorldConferences.net, 2013.

[6] T. Minegishi1 and A. Niimi, "Proposal of credit card fraudulent use detection by online type decision tree construction and verification of generality", International Journal for Information Security Research (IJISR), vol. 1, no. 4, 2011.

[7] 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.

[8] K.RamaKalyani and D.UmaDevi, "Fraud detection of credit card payment system by genetic algorithm", International Journal of Scienti_c Engineering Research, vol. 3, no. 7, 2012.

[9] 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.

[10] 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.

[11] 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.

[12] J. Pun and Y. Lawryshyn, “Improving credit card fraud detection using a metaclassification strategy,” International Journal of Computer Applications, vol. 56, no. 10 , 2012.

[13] R. Patidar and L. Sharma, “Credit card fraud detection using neural network,” International Journal of Soft Computing and Engineering (IJSCE), vol. 1, 2011.

[14] A. D. Pawar, P. N. Kalavadekar, and S. N.Tambe, “A survey on outlier detection technique for credit card fraud detection,” IOSR Journal of Computer Engineering (IOSRJCE), vol. 16, no. 2, 2014.

[15] 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.

[16] 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.

[17] G. Singh, R. Gupta, A. Rastogi, M. Chandel, and A. Riyaz, “A machine learning approach for detection of fraud based on svm,” International Journal of Scientific Engineering and Technology, vol. 1, no. 3, 2012.

[18] S. patel and S. Gond, “Supervised machine (svm) learning for credit card fraud detection,” International Journal of Engineering Trends and Technology (IJETT), vol. 8 , no. 3, 2014.

[19] A. Mukhopadhyay, S. Mukherjee, and A. Mahanti, “Artificial immune system for detecting online credit card frauds,” Research Front, CSI Communications, 2011.

[20] A. Srivastava, A. Kundu, and S. Sural, “Credit card fraud detection using hidden markov model,” IEEE Transactions On Dependable And Secure Computing, vol. 5, no. 1, 2008.

[21] G. Mhatre, O. Almeida, D. Mhatre, and P. Joshi, “Credit card fraud detection using hidden markov model,” International Journal of Computer Science and Information Technologies, vol. 5, no. 2, 2014.

[22] M. Z. Khan, J. D. Pathan, and A. H. E. Ahmed, “Credit card fraud detection system using hidden markov model and k-clustering,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 2, 2014.