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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

To Secure Online Payment System Using Steganography, Visual Cryptography and HMM

Amit R. Bramhecha, Prof. Dinesh D. Patil,

M. E, Dept. of Computer Engineering, SSGBCOE&T, Bhusawal, Maharashtra, India

HOD, Dept. of Computer Engineering, SSGBCOE&T, Bhusawal, Maharashtra, India

ABSTRACT: Over the last few years the number of small businesses processing payments, filling invoices and selling online has skyrocketed, along with the number of online payment providers. Typically, payment processing system providers use software as a service (SaaS) model and form single payment gateways for their clients to multiple payment methods. When users goes online to pay rent, dues, charges, or any donation, after selecting to pay by credit or debit card, the user passes on information such as name, credit or debit card details, and billing address, and then submits payment.

Online payment refers to money that is exchanged electronically. Typically, this involves use of computer networks, the internet and digital stored value systems. When you collect a payment over the internet, you are accepting an online payment and you are sharing your confidential card details with company.

This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby shielding customer data and increasing customer confidence and preventing identity theft. The approach uses combined application of Steganography, visual cryptography and HMM for this purpose.

I. INTRODUCTION

The most accepted online payment mode is credit/debit card for both online and offline in today's world, it provides cashless shopping at every shop in all countries. It will be the most convenient way to do online shopping for paying bills, purchasing etc. With access to the sensitive information that enables the exchange of billions of dollars in transactions each year, the payments infrastructure is a red-hot target for hackers.

Online money transfers and online banking save us a lot of time and make our lives easier. However, these same technologies also make life easier for cybercriminals by offering them new and easy ways to steal users' money. Using stolen payment data is an effective and popular way of making a quick profit. Although banks try to protect their customers, attacks against individual users are still quite common.

Merchants accepting online payments need to comply with a list of security requirements. The online payment specific security is designed to decrease the chance of the billing and personal information being stolen. The transfer needs to occur over secure encrypted connection. In the cases of recurring billing where customer data is stored, the merchant needs to enforce a longer list of security features and protocols that are usually referred to as PCI compliance requirements. Recurring billing systems that employ online payment procedures need to be periodically scanned for security vulnerabilities.

To accept an online payment the merchant needs to have access to an Online Payment Gateway. The online payment gateway is a service provider that is integrated with the credit card and transfers the online payment information between the merchant and the payment processor.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

The typical online payment process has the following stages:

1. Customer submits the payment information to the merchant. For example customer completes the payment form on the merchant website and submits the information.
2. The merchant submits the payment information to the online payment gateway.
3. The online payment gateway submits the payment to the payment processor.
4. The payment processor authorizes the payment and responds to the payment gateway
5. The payment gateway responds back to the merchant
6. The merchant responds back to the customer showing if the online payment was successful or not and taking the appropriate action.

An e-commerce online payment system facilitates the acceptance of electronic payment for online transactions. Also known as a sample of Electronic Data Interchange (EDI), e-commerce online payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking. A payment service provider (PSP) offers merchants online services for accepting electronic online payments by a variety of payment methods including credit card, bank-based payments such as direct debit, bank transfer, and real-time bank transfer based on online banking. An Internet Merchant Account (IMA) allows merchants to accept debit/credit card payments directly to their business bank account, online.

To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. In real life, fraudulent transaction are scattered with genuine transactions and simple pattern matching Techniques are not often sufficient to detect those frauds accurately.

The proposed system highlights a novel approach for creating a secure steganographic method and visual cryptography for data hiding in online payment. Although there has been an extensive research work in the past, but majority of the research work has no much optimal consideration for robust security towards the tet based encryption using steganography and visual cryptography. Since in this paper we are using Steganography mechanism for encrypting data, visual cryptography and HMM for detecting fraud if any one fraudster trying to misuse card information.

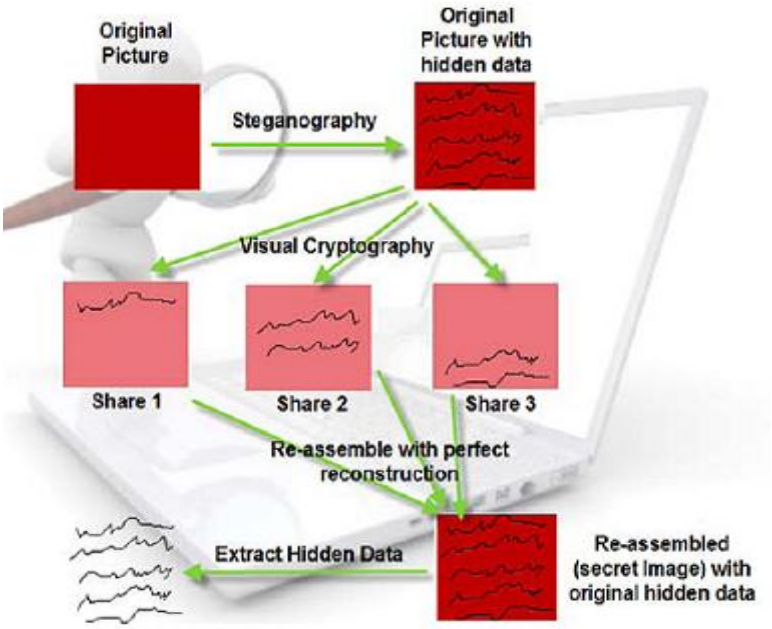

Fig1 : Overlapping of share 1, share 2 & share 3.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Steps of Executions:
In this developed approach, it contains mainly 3 modules to avoid phishing attack;
1. Data Steganography mechanism
2. Data Visual Cryptography
3. Hidden Markov Model

To prevent phishing attack:
Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

1. Steganography:
Text-Based Steganography: It makes use of features of English Language like inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a statement. The steganography program for each user is easy. It further protects against eavesdropping on the embedded information. It is most secured technique and provides high security.

2. Visual Cryptography
- Halftone visual cryptography: This novel technique achieves visual cryptography via half toning. Based on the blue -noise dithering principles, this method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information.
- 2-0ut-2 Visual Cryptography: Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process. This is equivalent to using the logical OR operation between the shares.

It is also proposed by Naor et al. in [4], is a cryptographic technique based on visual secret sharing used for image encryption.

3. Fraud Detection Methods:
The detection of fraud is a complex computational task and still there is no system that surely predicts any transaction as fraudulent. They just predict the likelihood of the transaction to be a fraudulent.

The properties of a good fraud detection system are:
1) It should identify the frauds accurately
2) It should detecting the frauds quickly
3) It should not classify a genuine transaction as fraud
In this paper, a comprehensive review of various fraud detection methods has been performed [3][4].

Hidden Markov Model (HMM):
Hidden Markov Model will be helpful to find out the fraudulent transaction by using spending profiles of user. It works on the user spending profiles which can be divided into major three types such as 1) Lower profile; 2) Middle profile; and 3) Higher profile. For every credit card, the spending profile is different, so it can figure out an inconsistency of user profile and try to find fraudulent transaction. It keeps record of spending profile of the card holder by both way, either offline or online. It can also be considered as the simplest dynamic Bayesian network[10].
Thus analysis of purchased commodities of cardholder will be a useful tool in fraud detection system and it is assuring way to check fraudulent transaction, although fraud detection system does not keep records of number of purchased goods and categories. Every user represented by specific patterns of set which containing information about last 10 transaction using credit card [4, 10].
The set of information contains spending profile of card holder, money spent in every transaction, the last purchase time, category of purchase etc. The potential threat for fraud detection will be a deviation from set of patterns.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

II. LITERATURE SURVEY

In paper [1] they proposed algorithm for credit card fraud detection named as BLAH. It Comprise of BLAST and SSAHA Algorithm. These algorithms are pretty much proficient sequence aligning algorithm in detecting credit card frauds. The system named as BLAHFDS identifies fraudulent transactions using a Profile Analyzer and a Deviation Analyzer. These two analyzers use BLAH as a sequence alignment tool to detect fraud. They proposed stochastic model for the generation of synthetic transactions to analyze the performance of BLAHFDS. Performance of this system in detecting fraud is good and its accuracy is high .also processing speed is Fast but it cannot detect the duplicate transaction or clone credit card frauds. BLASTSSAHA hybridization approach can be effectively used to counter fraud in other domains such as telecommunication.

In Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning, Paper [2], they proposed FDS Which Merges the result obtained from present and precedent behavior. The fraud detection system (FDS) consists of four Element: rule-based filter, Dempster–Shafer adder, transaction history database and Bayesian learner. Rule-based Filter extract the doubt level of each transaction based on variation from normal form of spending patterns. , Dempster–Shafer adder, in this component ,all the transaction that are doubtful obtained by rule based filter are combine to form primary belief.

Hidden Markov Model (HMM) is a popular statistical tool used by engineers and scientists to solve various problems. Ashphak Khan et al model the sequence of operations in processing of credit card transaction using HMM in which the transition probability related to hidden state and observations is considered [20]. M.Sasirekha et al propose an Intrusion Detection Systems (IDS) combining three approaches -anomaly, misuse and decision making model to produce better detection accuracy and a decreased false positive rate. The integrated IDS can be built to detect attacks in credit card system using HMM approach in the anomaly detection module. The credit card holder's behaviors are taken as attributes and the anomalous transactions are found by the spending profile of the user. The transactions that are considered to be irregular or abnormal are then sent to the misuse detection system. But before irregular use, it is difficult to restrict from misuse.

A customer authentication system using visual cryptography is presented in [12] but it is specifically designed for physical banking.
"New Visual Steganography Scheme for Secure Banking Application" [14] proposes a combined image based steganography and visual cryptography authentication system for customer authentication in core banking. But its having constrain of core banking where physically user should be present. Since in our system is superior than existing where we are using combination of 3 mechanism for restricting misuse of card information's as well as detection of misuse Steganography, Visual Cryptography and HMM. Steganography and Visual Cryptography are using for encrypting information while making online payment.

HMM is used for restricting even information is hacked by hacker. We are able to provide different cluster information to HMM model for detecting misuse like different transaction attributes location of transaction, amount of transaction, category of items etc.

III. PROPOSED SYSTEM

The proposed work is basically a framework designed in C# with three modules e.g. Steganography using Genetic Algorithm, Visual Cryptography and HMM[9][10]. System implementation can see in following figure 2.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

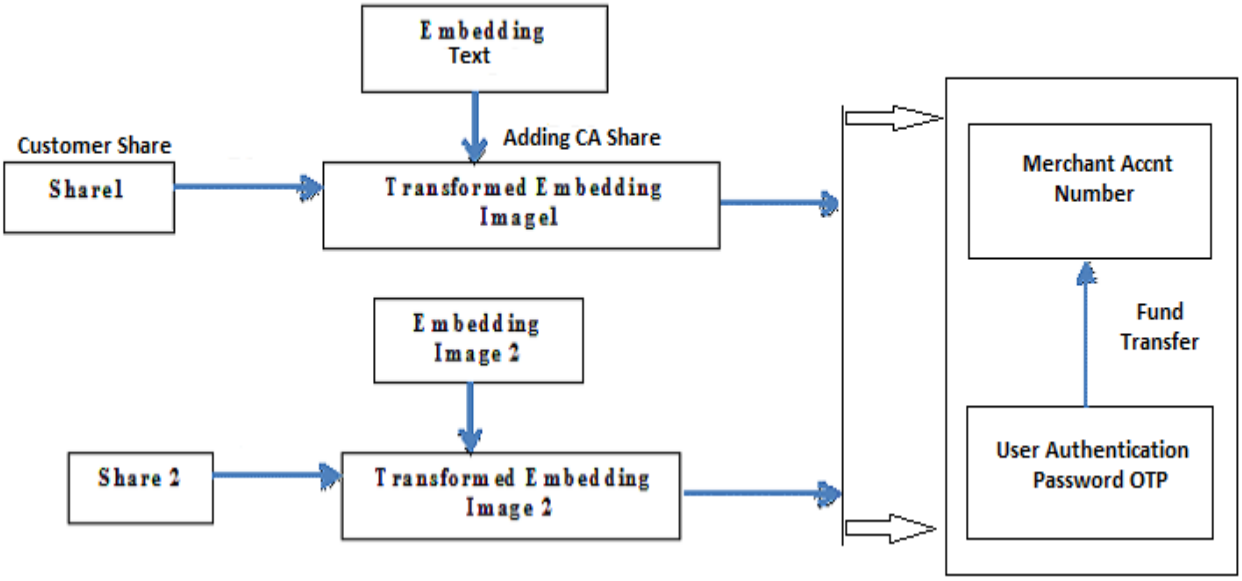

Fig2: Implementation of System.

The steganography technique is based on Vedic Numeric Code [11] in which coding is based on tongue position. For applying the Vedic code to English alphabet, frequency of letters in English vocabulary [18] is used as the basis for assigning numbers to the letters in English alphabet.

An input text is accepted for the input message in plain text format. After embedding the secret message in LSB (least significant bit) of the cover image, the pixel values of the steg-image are modified by the visual cryptography to keep their statistic characters. The experimental results should prove the proposed algorithm's effectiveness in resistance to steganalysis with better visual quality. The user can select their targeted information in terms of plain text for embedding the secret message in LSB of the cover image. LSB steganography has low computation complexity and high embedding capacity, in which a secret binary sequence is used to replace the least significant bits of the host medium. This is also one of the strong algorithms which keeps the information proof from any intruder.
In Visual Cryptography input is Stego-Image and Output will be Encrypted Shares.

Algorithm: Visual Cryptography
1 Read Stego-Image generated
2. The stego image is breaked into three layers namely split-1, split-2, split-3 these three files are containing the hidden data and to get the hidden data these three files have to be reconstructed perfectly then
3. The re-assembled picture and the extracted data will be gained again.
The proposed scheme is based on standard visual cryptography as well as visual secret sharing. The applied technique uses allocation of pseudorandom number as well as exchange of pixels. One of the contrast part of this implementation is that while decrypting, the stego-image will be morphologically same compared to the cover image with respect to the shape and size thereby preventing pixel expansion effect.

The implementation of the algorithm yields in better result with insignificant shares when stego images are normally with light contrast. It can also be seen that the algorithm gives much darker shares in both gray as well as colored output.
The stego-image generated from the steganographic module will be then subjected to our visual cryptography module which generates 3 secret shares as shown in Fig 3.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

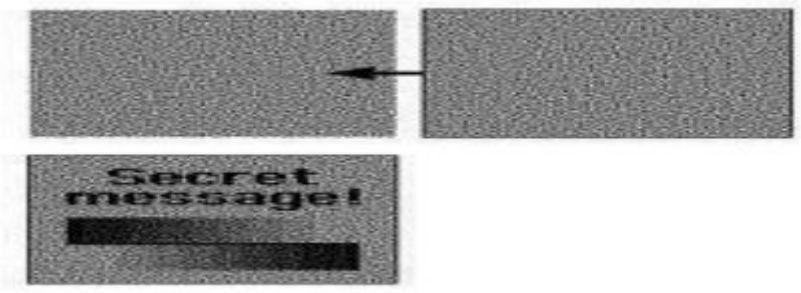

Fig 3: Visual Cryptography

HMM System Description:

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.

In this prediction process, HMM consider mainly three price value ranges such as,

1) Low (l),

2) Medium (m) and,

3) High (h).

As business processing of credit card fraud detection system runs on a credit card issuing bank site or merchant site. Each arriving transaction is submitted to the fraud detection system for verification purpose [05]. The fraud detection system accept the card details such as credit card number, cvv number, card type, expiry date and the amount of items purchase to validate, whether the transaction is genuine or not [06]. The implementation techniques of Hidden Markov Model in order to detect fraud transaction through credit cards, it create clusters of training set and identify the spending profile of cardholder [6].

The number of items purchased, types of items that are bought in a particular transaction are not known to the Fraud Detection system, but it only concentrates on the amount of item purchased and use for further processing [08].

It stores data of different amount of transactions in form of clusters depending on transaction amount which will be either in low, medium or high value ranges.

IV. TECHNIQUES AND ALGORITHM USED

To record the credit card transaction dispensation process in conditions of a Hidden Markov Model (HMM), it creates through original deciding the inspection symbols in our representation. We quantize the purchase values x into M price ranges V_1, V_2 . . . V_M, form the study symbols by the side of the issuing bank [07]. The genuine price variety for each symbol is configurable based on the expenditure routine of personal cardholders.

HMM determine these prices rang dynamically by using clustering algorithms (like K clustering algorithm) on the price values of every card holder transactions. It uses cluster V_k for clustering algorithm as k ¼ 1, 2 . . . . M, which can be represented both observations on price value symbols as well as on price value range [06].

In this prediction process it considers mainly three price value ranges such as 1) low (l) 2) Medium (m) and 3) High (h). So set of this model prediction symbols is V { l, m, h}, so V ¼ f as l (low), m (medium), h (high) which makes M ¼ 3. E.g.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

If card holder perform a transaction as $ 250 and card holders profile groups as l (low) = (0, $ 100], m (medium) = ($ 200, $ 500], and h (high) = ($ 500, up to credit card limit], then transaction which card holder want to do will come in medium profile group. So the corresponding profile group or symbol is M and V (2) will be used.

We are also finding out Threshold limit value (TLV) for detecting unusual transaction and to detect fraud in transaction. TLV Boundary beyond which a radically different state of affairs exists. Here we are asking to user to feed up Threshold value for more security to online payment.

In various period of time, purchase of various types with the different amount would make by credit card holder. It uses the deviation in a purchasing amount of latest 10 transaction sequence (and adding one new transaction in that sequence) which is one of the possibilities related to the probability calculation.

In initial stage, model does not have data of last 10 transactions, in that case, model will ask to the cardholder to feed basic information during transaction about the cardholder such as mother name, place of birth, mailing address, email id etc. Due to feeding of information, HMM model acquired relative data of transaction for further verification of transaction on spending profile of cardholder.
Fig 4 shows the systems training set for calculating Threshold value at run time. System's security checking you can see in following fig 5.

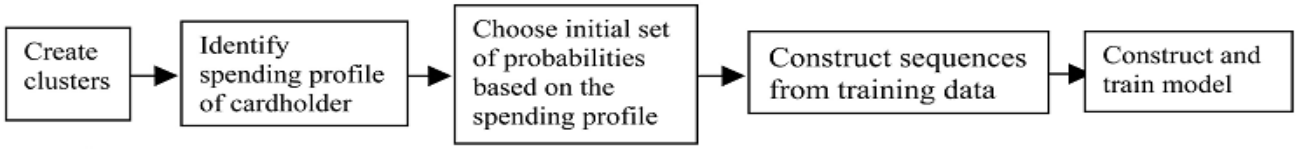

Fig4: Training for calculating Threshold value at run time.

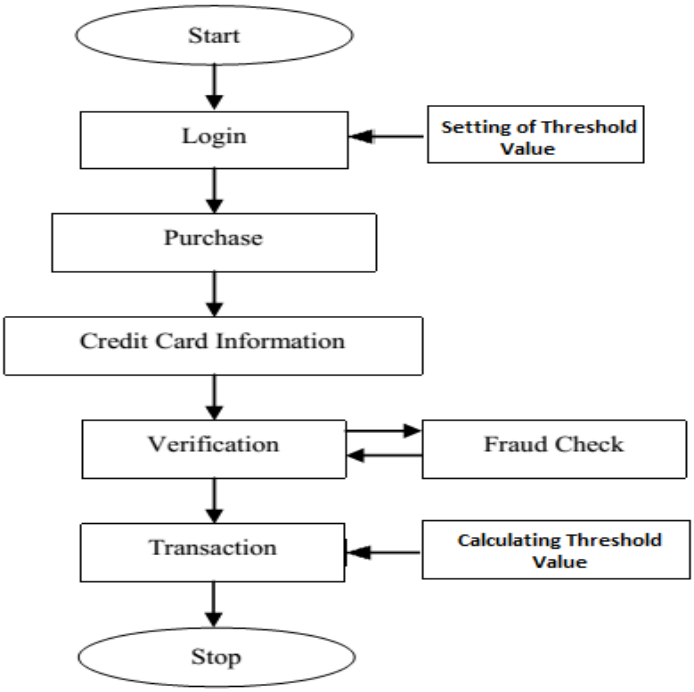

Fig4: HMM Module for security checking while transaction.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Threshold value:
In Transaction Alert, we are defining threshold value for maintaining online payment security for avoiding fraud while transaction. This is added security measure that we are providing by using HMM. In HMM we are calculating Threshold value of all transaction. If it is initial transaction for new card holder then user can provide threshold value explicitly. Since if any one exceeding that limit, it will generate alert which will be given to the genuine card holder and those are doing fraud that transaction will be cancelled.

The bank will send you a Transaction Alert via SMS. You may log in to Online Banking to change the threshold value. This alert serves as a fraud prevention measure and you should immediately contact the bank if the transaction was not authorized by you.

OTP (One-Time Password) for secure online transactions:
At the same time a One-Time Password (OTP) will be sent to the mobile phone registered with us for completion of online transactions made at merchant. This provides an additional layer of authentication during the transaction. So even someone stolen cardholders information and making fraud, doing some transaction, it require OTP password also.
In this section, it is shown that fraud detection will be checked on last 10 transactions and also calculate percentage of each spending profile (low, medium and high) based on total number of transactions. In Table 1, list of all transactions are shown. Table 1, list of all transactions happened till date.

No. of Transaction	Amount	No. of Transaction	Amount
1	1000	11	600
2	1200	12	1000
3	1400	13	1400
4	800	14	1100
5	1000	15	800
6	1500	16	10000
7	1300	17	1600
8	2000	18	2000
9	3000	19	1500
10	5000	20	600

Table 1: Online Transaction details

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

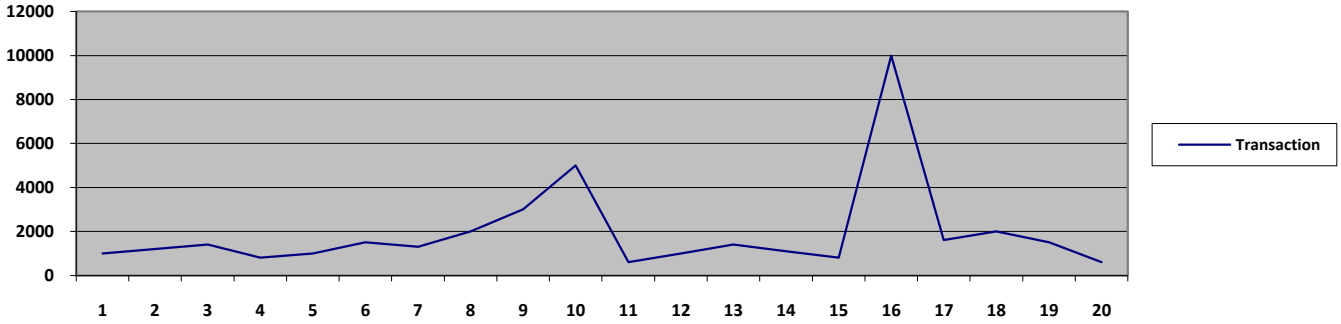

Fig: 2-D Transactions data and its threshold value.

For finding out threshold value, we have to find out mean value by considering first 5 transactions.
Mean Value (Threshold Value) $M_V = (T_1+T_2+\cdots+T_n) / N$
where T is transactions and N is number of transaction. After getting M_V value, we are comparing it with every transaction and if bigger amount is greater than that difference then it will generate alert.
Here, u can consider table 1 for finding out Threshold value $\mathbf{M_V}$.

Threshold Value= (1000+1200+1400+800+1000)/5 = 1080.
So system will calculate difference between current transaction and Threshold value and it will generate appropriate alert for user. If it is fraud, user will get alert and that transaction will get cancelled. If bigger amount transaction is done by user then user has to give OTP to complete transaction.

No. of Transaction	Amount	Difference Value	Alert (Yes/No)	No. of Transaction	Amount	Difference Value	Alert (Yes/No)
1	1000	-80	No	11	600	-480	No
2	1200	120	No	12	1000	-80	No
3	1400	320	No	13	1400	320	No
4	800	-400	No	14	1100	20	No
5	1000	-80	No	15	800	-280	No
6	1500	420	No	16	10000	8920	Yes
7	1300	220	No	17	1600	520	No
8	2000	920	No	18	2000	920	No
9	3000	1920	Yes	19	1500	420	No
10	5000	3920	Yes	20	600	-480	No

For Ex. T1-1080= -80, T2-1080= 120…
The most recent transaction is placed at the first position and correspondingly first transaction is placed at the last position in the table.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

The pattern of spending profile of the card holder is shown in Figure 2 based on all transactions done. Here threshold value is 1080 so above 1080, all transaction are in high risk. So it's almost 15% high risk transaction and that can easily detectable and once they get detected by system it will get rejected.

V. CONCLUSION

The developed system has discussed implementation of securely using steganograph, Visual Cryptography and HMM techniques. So we are restricting to the merchant to misuse of cardholders data and making fraud transactions. We have also effectively used the HMM technique for finding out user's transaction patterns at run time if someone doing fraud by using user information.
In that case alert will generate alert and transaction will not be complete until and unless user will not provide OTP. So HMM can detect whether an incoming transaction is fraudulent or not.
This mechanism is useful for every kind of E-commerce business. Table shows how we can find out threshold value and by using it, how we can avoids phishing attacks. So by using triple layer steganograph, Visual Cryptography and HMM security we are able to provide more security in online transaction.

ACKNOWLEDGMENTS

It is my great pleasure to express my deep sense of gratitude to my project guide Prof. Dinesh D. Patil, Head of Computer Department for his valuable guidance, inspiration and wholehearted involvement during every stage of this paper presentation.
I am very much grateful to the entire SSGBCOE&T Bhusawal for giving me all facilities and work environment which enable me to complete my task.

REFERENCES

1. Ashphak Khan, Tejpal Singh, AmitSinhal, "Observation Probability in Hidden Markov Model for Credit Card Fraudulent Detection System", Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28- 30, 2012.
2. Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, ―Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning, Special Issue on Information Fusion in Computer Security, Vol. 10, Issue no 4, pp.354- 363, October 2009.
3. P.K. Chan, W. Fan, A.L. Prodromidis, S.J. Stolfo "Distributed Data Mining in Credit Card Fraud Detection". Data Mining; (1999). (67–74).
4. Phua, C, Lee, V., Smith, K., Gayler, R "A comprehensive survey of data mining-based fraud detection research". Artificial Intelligence Review. (2002).
5. R.C. Chen, T.S. Chen, C.C. Lin ("A new binary support vector system for increasing detection rate of credit card fraud". International Journal of Pattern Recognition 2006). 20 (2); (227–239).
6. Phua, C., Lee, V., Smith, K., and Gayler, R., 2007. A Comprehensive Survey of Data Mining-Based Fraud Detection Research (2007), March.
7. Rabiner, L.R. 1989. A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition, Proceedings of IEEE, vol. 77, no. 2 (1989), pp.257-286.
8. Ourston, D., Matzner, S., Stump, W., and Hopkins, B., 2003. Applications of Hidden Markov Models to Detecting MultiStage Network Attacks, Proceedings of 36th Annual Hawaii International Conference System Sciences, vol. 9 (2003), pp. 334-344.
9. Cho, S.B., and Park, H.J., 2003. Efficient Anomaly Detection by Modeling Privilege Flows Using Hidden Markov Model, Computer and Security, vol. 22, no. 1 (2003), pp. 45-55.
10. Kim, M.J., and Kim, T.S., 2002. A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection, Proceedings of International Conference on Intelligent Data Eng. and Automated Learning, (2002), pp. 378-383.
11. Souvik Roy, P. Venkateswaran "Online Payment System using Steganography and Visual Cryptography" 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science.
12. Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.
13. Abhinav Srivastava, Amlan Kundu, Shamik Sural "Credit Card Fraud Detection Using Hidden Markov Model" IEEE Transactions On Dependable And Secure Computing, Vol. 5, No. 1, January-March 2008.
14. S.Premkumar, A.E.Narayanan, "New Visual Steganography Scheme for Secure Banking Application," Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 – 1016, Kumaracoil, India, 2012.
15. Bharati Krishna Tirthaji, "Vedic Mathematics and its Spiritual Dimension," Motilal Bansari Publishers,1992.
16. Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shopping online," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011.
17. "Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics" IJCSIT, Vol. 3 (3) , 2012,4366 – 4370.
18. Hu ShengDun, U. KinTak, "A Novel Video Steganography Based on Non-uniform Rectangular Partition," Proceding of 14th International Conference on Computational Science and Engineering, pp. 57-61, Dalian, Liaoning, 2011.
19. R. Chandramouli, Nasir Menon, Analysis of LSB Based Image Steganography techniques, IEEE-2001.
20. Ashphak Khan, Tejpal Singh, AmitSinhal, "Observation Probability in Hidden Markov Model for Credit Card Fraudulent Detection System", Proceedings of the Second International Conference on Soft Computing for Problem Solving (SocProS 2012), December 28- 30, 2012.