International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

Online Payment System Using Steganography and Visual Cryptography

[1] Sumana Sarkar [2] Srinivas Goud, [3] Prasad B
[1]II/IV, [2][3]Associate Professor
[1][2][3] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM) Hyderabad
[1] sumanasarkar1995@gmail.com [2] sree.srinu@mlritm.ac.in[3]bprasad@gmail.com

Abstract: **This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby safe guarding customer data and increasing customer confidence and preventing identity theft. In recent time there is rapid growth in E-Commerce market. Major concerns for customers in online shopping are debit card or credit card fraud and personal information security. Identity theft and phishing are common threats of online shopping. The approach uses combined application of BPCS Steganography and visual cryptography for this purpose. Payment portal, a channel between consumers and payment processors, use numerous security tools to secure a consumer's payment information, ordinarily card data, during an online transaction. Moreover, not all merchants provide a secure payment environment to their consumers and, in spite of having a standard payment plan, adhere to it. Consequently, this exposes a consumer's payment information to risks of being compromised or misused by merchants or stolen by hackers and spammers.**

Keywords: **Customer confidence, Preventing identity theft, E-Commerce market, Information security, Steganography, Visual cryptography, Payment portal.**

I. INTRODUCTION

Problem Definition:
Phishing is a criminal mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others.

Existing System:
Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks.Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant**.** A customer authentication system using visual cryptography is presented , but it is specifically designed for physical banking.A signature in but it also requires physical presence of based authentication system for core banking is proposed the customer presenting the share.A biometrics in conjunction with visual cryptography is used as authentication systemDoes not provide a friendly environment to encrypt or decrypt the data (images). Not suitable for online paymentsIt is expansive of Using biometrics

Disadvantage of Existing System:
In result to hide 4 letter word, 8 words are required excluding the words that are added to provide flexibility in sentence construction. So to hide a large message, this technique requires large no of words and creates a complexity in sentence construction. Disadvantage of this technique can be used in its advantage by applying it to online banking to create spam mail to hide one's banking information.

Proposed System:
In the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of Steganography and visual cryptography. The information received by the merchant can be in the form of account number

related to the card used for shopping. The information will only validate receipt of payment from authentic customer.

Advantage of Proposed System:
Proposed method minimizes customer information sent transfer of fund to the online merchant. So in case of a breach in merchant's database, customer doesn't get affected. It also prevents unlawful use of customer information at merchant's side. Presence of a fourth party, CA, enhances customer's satisfaction and security further as number of parties are involved in the process. Usage of Steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy. Cover text can be sent in the form of email from CA to bank to avoid rising suspicion. Since customer data is distributed over 3 parties, a breach in single database can easily be contented**.**

II. MODULES

The mentioned are the modules for the existing system Steganography, Encoding, Decoding, Tranction Online Shoping, Customer Authentication, Certificate Autority Acess, Final Authentication.

Steganography:
In this module, Steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a sentence. This gives flexibility and freedom from the point view of sentence construction but it increases computational complexity.

Encoding:
- Representation of each letter in secret message by its equivalent ASCII code.
- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts.
- Choosing of suitable letters from table 1 corresponding to the 4 bit parts.
- Meaningful sentence construction by using letters obtained as the first letters of suitable words.
- Encoding is not case sensitive.

Decoding:
- First letter in each word of cover message is taken and represented by corresponding 4 bit number.
- 4 bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

Tranction Online Shoping:
In this module traditional online shopping consumer selects items from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of third party payment systems such as PayPal, pay online system, Web Money and others. In the payment portal consumer submit his or her credit or debit card details such as credit or debit card number, name on the card, expiry date of the card.

Customer Authentication:
Customer unique authentication password in connection to the bank is hidden inside a cover text using the text based Steganography method. Customer authentication information (account no) in connection with merchant is placed above the cover text in its original form. Now a snapshot of two texts is taken. From the snapshot image, two shares are generated using visual cryptography. Now one share is kept by the customer and the other share is kept in the database of the certified authority.

Certificate Autority Acess:
During shopping online, after selection of desired item and adding it to the cart, preferred payment system of the merchant directs the customer to the Certified Authority portal. In the portal, shopper submits its own share and merchant submits its own account details. Now the CA combines its own share with shopper's share and obtains the original image. From CA now, merchant account details, cover text are sent to the bank where customer authentication password is recovered from the cover text.

Final Authentication :
Customer authentication information is sent to the merchant by CA. Upon receiving customer authentication password, bank matches it with its own database and after verifying legitimate customer, transfers fund from the customer account to the submitted merchant account. After receiving the fund, merchant's payment system validates receipt of payment using customer authentication information.

III. SYSTEM DESIGN

The DFD diagram for the proposed system is shown in fig 1.

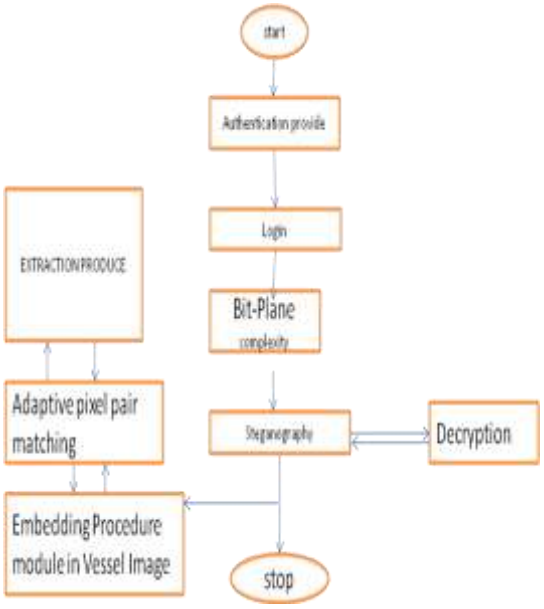

Fig 1: DFD diagram

IV. SYSTEM IMPLEMENTATION

Fig 2: Admin's Login Page

In this page the admin login and check all total database or any new users request are been thereto be added in this page as shown in the fig 2.

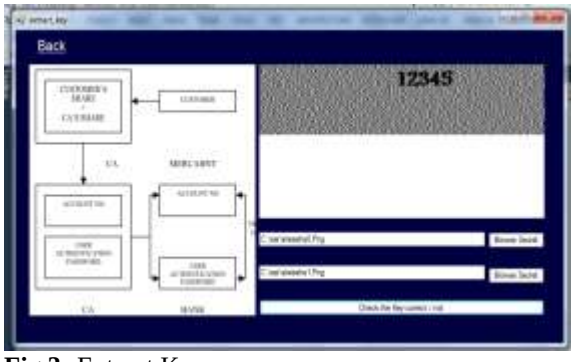

Fig 3: Extract Key

In this page the user browse their secret image to upload in their data base as shown in the fig 3.

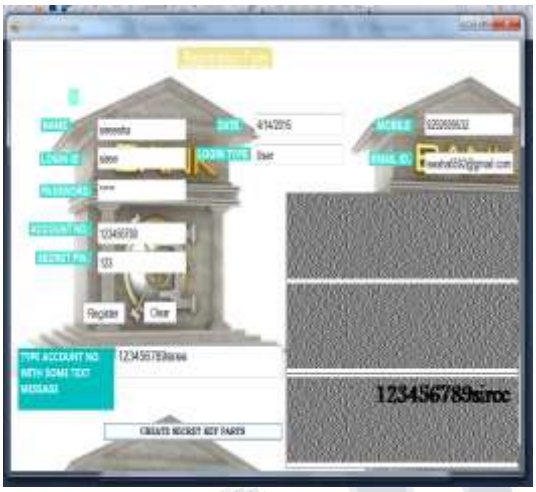

Fig4: Registration of Users

In this page the user getting registers by filling the personal details as shown in the fig 4.

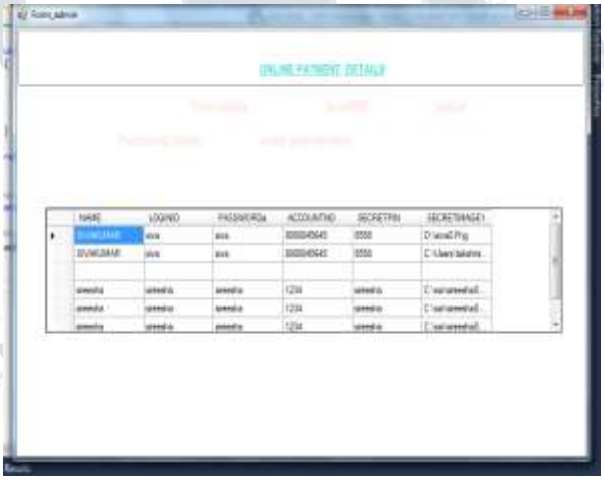

Fig 5: Form Admin' S

In this page the admin check the total number of users and their data base as shown in the fig 5.

Fig 6: Sent SMS

In this page the user who all got register any notification to the user will be send through this sms as shown in the fig 6.

Fig 7: Login to Transfer Fund

In this page the user getting Login to transfer Fund by filling his name, login Id, Password as shown in the fig 7.

Fig 7: Transfer Fund

In this page the user login to transfer fund after giving their details of a user and the secret image of user and admin one should match then only transaction will be success as shown in the fig 7.

Fig 8: Transfer Fund in Process

In this page after matching of secret image the fund is been processed and the user can purchase the product as shown in the fig 8.

Fig 8 : Shopping Store

In this the user can buy the things which are in store and order it as shown in the fig 8.

V. CONCLUSION

In this paper, a payment system for online shopping is proposed by combining text based Steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. The method is concerned only with prevention of identity theft and customer data security. In comparison to other banking application which uses Steganography and visual cryptography are basically applied for physical banking, the proposed method can be applied for E-Commerce with focus area on

payment during online shopping as well as physical banking.

REFERENCES

[1] 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

[2] Javelin Strategy & Research, "2013 Identify Fraud Report," https://www.javelinstrategy.com/brochure/276.

[3] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report,2013,"http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf .

[4] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, "Hiding Information in Document Images," Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489, 1995.

[5] J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2003.

[6] 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.

[7] Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding," Proceedings of the First International Workshop on Information Hidding, pp. 293- 315, Cambridge, UK, 1996.

[8] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313- 336, 1996.

[9] K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text," Purdue University, Cerias Tech Report 2004—2013.

[10] J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.

[11] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.

[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] Chetana Hegde, S. Manu, P. Deepa Shenoy, K. R. Venugopal, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications," Proceedings of 16th International Conference on Advanced Computing and Communications, pp. 65-72, Chennai, India, 2008