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. 4, Issue 3, March 2016

Survey on Online Payment System using Steganography and Visual Cryptography

Ganesh D. Patil[1], Sandip B. Mhaske[1], Usha Khamkar[1], Sujata B.Alhat[1], Prof. Kanif S. Hirve[2]

B. E Student, Department of Computer, HSBPVT's COE, Kashti, Ahmednagar, Maharashtra, India[1]

Assistant Professor, Department of Computer, HSBPVT's COE, Kashti, Ahmednagar, Maharashtra, India[2]

ABSTRACT: Now a days E-commerce is growing fast in the world. With this popularity debit card and credit card fraud increasing rapidly so personal information security is major concern for merchants, persons and banks specifically in the case of CNP (Card NotPresent). In these studies we are providing limited data for the online shopping which is secure own information and safeguard for customers andincreasing customer confidence and preventing identity theft.The method uses combined application of steganography andvisual cryptography for this purpose.

KEYWORDS: Information security; Steganography; VisualCryptography; online shopping.

I. INTRODUCTION

In Online shopping search product information online retrieve information about product and for purchase these product need to be provided credit or debit card information online. Product delivered online on registered address. In online shopping Identity theft and phishing are the common dangers of online shopping. Stolen someone's personal information is known as Identity theft and misuse of that information for making purchase and opening of bank accounts or arranging credit cards. In 2012 consumer information was misused for an average of 48 days as a result of identity theft [2]. Phishing is a criminal mechanism that employs social and technical information stolen and steal consumer's personal identity and financial account credentials. In second half of 2013, Most of the phishing attack done in financial, retails and payment services [3].Bank information will not secure in online. To cure these issue secure socket layer will help. SSL Secure Socket Layer encryption will prevent the transmission of personal data in between consumer and online merchants or any phishers. 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. In these studies we are proposed one method text based steganography and visual cryptography which is based on minimum information and required information share online between consumer and online merchant for the personal information security but able to transfer fund to the merchant and prevent the misuse of information from merchant side. The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking. Online shopping also called as e-tail is a way of purchasing products over internet. It allows customers to buy goods or services using web browsers and by filling credit or debit card information . In online shopping the common threats are phishing and identity theft. Identity theft is a form of stealing someone's identity i.e. personal information in which someone pretends to be someone else. The person misuses personal information for purchasing or for opening bank accounts and arranging credit cards. As a result of identity theft, the customer's information was misused for an average of 48 days in 2012. Phishing is a method of stealing personal confidential information such as username, passwords, and credit card details from victims. It is a criminal mechanism that uses social engineering. Phishing email directs the users to visit website where they take users personal information such as bank account number, password. It is email fraud conducted for identity theft. In 2013, Financial and Retail Service, Payment service are the targeted industrial sectors of phishing attacks.

II. RELATED WORK

An A brief survey of related work in the area of banking security based on steganography and visual cryptography is presented in this section. A customer authentication system using visual cryptography which is used mostly in physical

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. 4, Issue 3, March 2016

banking. For core banking signature based system is proposes in system but it will required consumer presenting the share. A combined image based steganography and visual cryptography authentication system for customer authentication in core banking. The image algorithms help for the prevent fraud in E-Banking.

In this system there will be two servers, bank server (admin) and merchant server (product admin). Product admin will add the products and product related information in its database. Admin i.e. bank server will add users and merchant servers. User specific data includes user name, user id, transaction password and user password. While merchant server specific data includes server id, password and URL in the Admin's database. Client will select the product and log in to respective site. Then verification request is sent to merchant server. Merchant server will verify the user name, user id and along with that it will add server id, server key and send it to the bank server for the verification. Bank server will verify the server id, server key of merchant server. If it is ok then bank server will generate one OTP through steganography. If the merchant server is fake then it will not generate OTP. After OTP generation it will form two shares using visual cryptography. One will be sent to the client via email and other will be sent to the merchant server. Merchant server will send the second share to the client. After having two shares, at client side these two shares are combined and original OTP gets generate.

In phase 1, bank server will communicate with merchant server by sending share1 to the merchant server. In phase 2, bank server will communicate with client by sending share2 to the client. In third phase, there is communication between merchant server and client and original OTP gets generated by combining share1 and share2 at client side. In fourth phase, if the generated OTP is valid then required transaction will be carried out.

III. 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. As using text based steganography customer get one unique id which is hidden in text this authentication password connected with the bank. These unique authentication id connected with merchant in his place with original form.

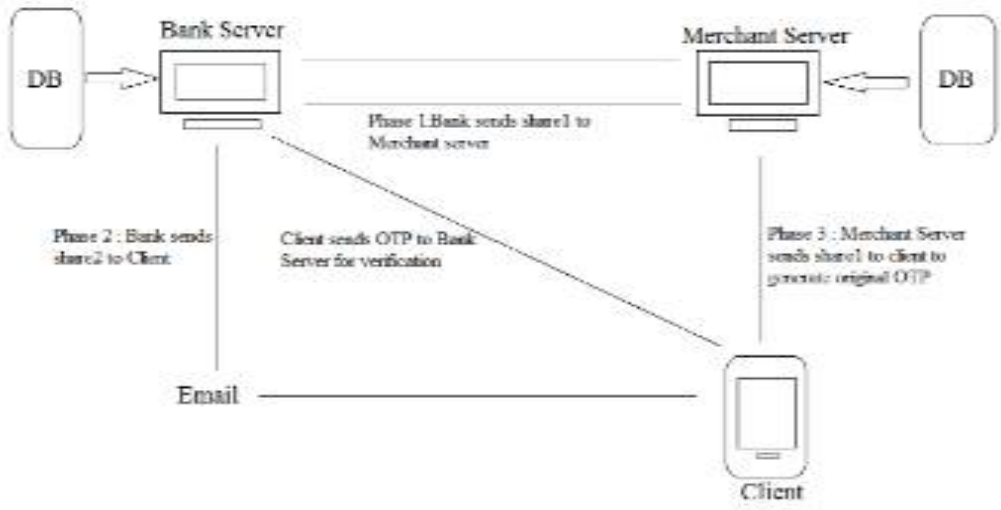

Fig. 1 System Architecture

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. On the time of online shopping when customer select product that time payment service can direct with customer to the

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. 4, Issue 3, March 2016

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. Now cover text and merchant details will be sent to the bank where customer authentication text retrieve from the cover text then these information send to the merchant by CA. On the basis of customer authentication password bank matches the with own data base, verify customer then transfer fund customer account to merchant account After receiving the fund, merchant's payment system validates receipt of payment using customer authentication information. The problem is that CA does not know to which bank to forward the cover text obtained from combining two shares. It can be solved by appending 9 digit routing or transit number of bank with customer authentication information. If "text" is customer unique authentication password and account no of customer is 12345678910111, snapshot of cover text and account no is shown in Fig. 2 and resultant shares by the application of visual cryptography.

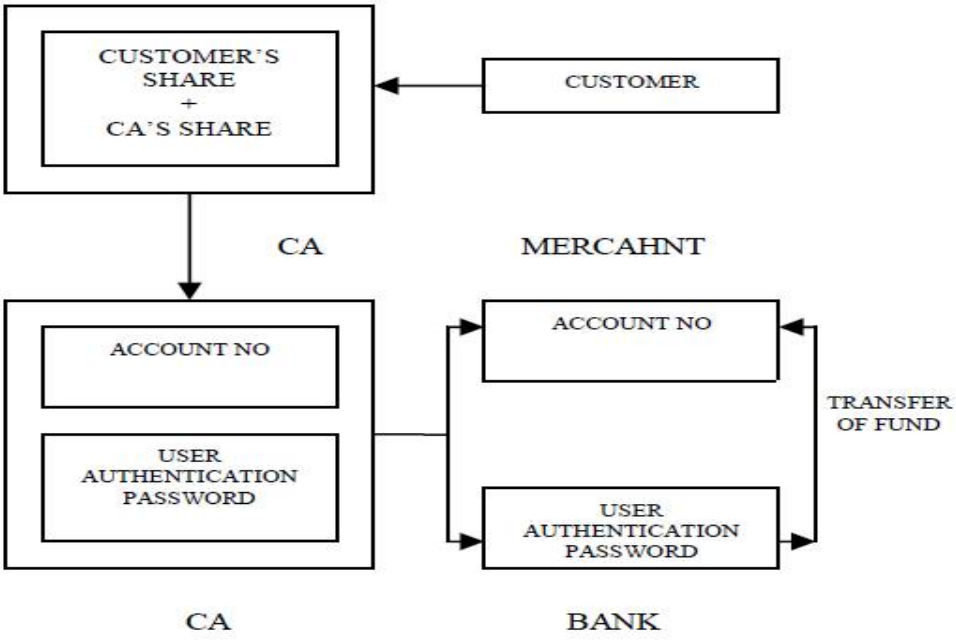

Fig.2 System Flow

A. Advantage

Proposed method minimizes customer information sent 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 atmerchant's side.

- Presence of a fourth party, CA, enhances customer'ssatisfaction and security further as more number ofparties are involved in the process.
- Usage of steganography ensures that the CA does not know customer authentication password thusmaintaining customer privacy.
- Cover text can be sent in the form of email from CA tobank to avoid rising suspicion.
- Since customer data is distributed over 3 parties, abreach in single database can easily be contented

B. Security threat

- During payment, merchant's payment system requiresto direct the shopper to CA's portal but fraudulentmerchant may direct shopper to a portal similar to CA'sportal but of its own making and get hold of customerown share. To prevent this type of phishing attack, anend-host based approach can be implemented fordetection and prevention of phishing attack as in [22].

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. 4, Issue 3, March 2016

C. Method Extension

- The payment system can also be extended to physicalbanking. Shares may contain customer image orsignature in addition to customer authenticationpassword. In the bank, customer submits its own shareand customer physical signature is validated against thesignature obtained by combining customer's share andCA's share along with validation of customerauthentication password. It prevents misuse of stolencard and stops illegitimate customer.

IV. 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. Z. Jihui Chen, XiaoyaoXie, 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.Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report,2013,"http://docs.apwg.org/reports/apwg_trends_report_q2_2013 .
3. 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.
4. 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.
5. 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.
6. Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding," Proceedings of the First International Workshop on Information Hidding, pp. 293- 315, Cambridge, UK, 1996.
7. Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313- 336, 1996.
8. K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text," Purdue University, Cerias Tech Report 2004—2013.
9. J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.

.

BIOGRAPHY

Mr. Ganesh D. Patil, is Student at Computer Department, HSBPVT's COE, Kashti, Ahmednagar, Maharashtra
Mr.Sandip B. Mhaske is Student at Computer Department, HSBPVT's COE, Kashti, Ahmednagar, Maharashtra
Miss. UshaKhamkar is Student at Computer Department, HSBPVT's COE, Kashti, Ahmednagar, Maharashtra
Miss. Sujata B. Alhat is Student at Computer Department, HSBPVT's COE, Kashti, Ahmednagar, Maharashtra
Prof.Kanif S. Hirve is Assistant Professor at Computer Department, HSBPVT's COE, Kashti, Ahmednagar, Maharashtra