Volume 3, Issue 4, April-2016, pp. 157-161 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Online Payment System using Steganography and Visual Cryptography

[1]Priyanka More,[2] Pooja Tiwari, [3]Leena Waingankar, [4]Vivek Kumar,[5]A. M. Bagul

Department of Computer Engineering, NBN Sinhgad School of Engineering
Savitribai Phule Pune University, Pune-411041, India
(morepriyanka66@yahoo.com, poojakt123@gmail.com)

Abstract: - 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. Phishing is a method of stealing personal confidential information such as username, passwords and credit card details from victims. It is a social engineering technique used to deceive users. In this paper new method is proposed that uses text based steganography and visual cryptography. It represents new approach which will provide limited information for fund transfer. This method secures the customer's data and increases customer's confidence and prevents identity theft.

Keywords – Steganography; Visual Cryptography; online shopping; Phishing

1. INTRODUCTION

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. 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.

The method which is proposed in this paper uses both steganography and visual cryptography. It reduces information sharing between customer and merchant server and safeguards customers' information. It enables successful fund transfer to merchant's account from customer's account and prevent misuse of information at merchant side. In this system there are two shares of OTP which are combined to get original OTP. In this way the system provides secure transaction.

The rest of the paper includes: Section II describes steganography and visual cryptography. Section III gives brief idea of transaction in online shopping. Section IV includes merchant and bank server. Section V gives steganography and visual cryptography

algorithm. Section VIproposed payment system. Section VII gives advantages. Section VII gives conclusion of the paper.

II.STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Steganography is the art of hiding of a message within another message. It is a technique of hiding the information into the image. . Steganography made of the two words steganos and graphein. Steganos means covered or protected and the meaning of graphein is writing. The basic concept behind steganography is that message to be transmitted is not detectable to casual eye. Steganography technique uses text, image,and video, audio as a cover media for hiding data. The hidden message may be in invisible link between the visible lines of personal letter. Number of words, number of characters, number of vowels, and position of vowels in a word are also used to hide the message. A text steganography technique requires small memory and simpler communication. At transport layer, electronic communication involves steganography coding.

Cryptography is the study of techniques for secure communication in the presence of third party. It is special encryption technique in which visual information is encrypted in such a way that decryption does not require a computer. Moni Naor and Adi Shamir developed this technique. It was developed in year 1994. Visual cryptography contains two transparent images. One image contains random pixels and another image contains secret information. It is impossible to retrieve secret information from one of the images. The two images are required to retrieve the correct information.

III.TRANSACTION IN ONLINE SHOPPING

In online shopping customer selects products from online shopping portal and then customer is directed to the payment page. Online merchant may use third party payment systems such as PayPal, Web Money and others or online merchant may use its own payment system. In Online payment portal customer submits his or her credit or debit card details such as credit or debit card number, name on the card, expiry date of the card.

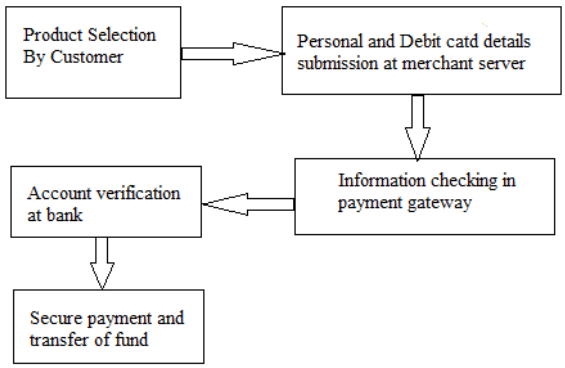

Figure 1. Transaction in online shopping.

Details of information given to online merchant vary from one payment gateway to another. Payment in IRCTC website requires Personal Identification Number (PIN) if you are using debit card for payment whereas shopping in Flipkart or Snapdeal requires Visa or Master secure code. Online merchant may require a Card Verification Value code, CVV (CVV2 for Visa, CVC2 for MasterCard).CVV is basically an authorizing code in CNP transactions. According to the PCI Data Security Standard [20], merchants are not allowed to store CVV information or PIN data. Online merchant can store card information such as name, card number and expiration date.

IV. MERCHANT AND BANK SERVER

In this paper there is one admin application and one product admin. The functionality of admin application is to add the servers and users. It also manages added servers and users. There can be n number of users but only two servers we are using i.e. one merchant server and one is fake server. There is client application is also available. The main aim of product admin is to add various categories and different products into that category. The client application is an android application. Basically client accesses the various products present at merchant server via android application.
The connectivity between client, merchant and bank server is shown below.

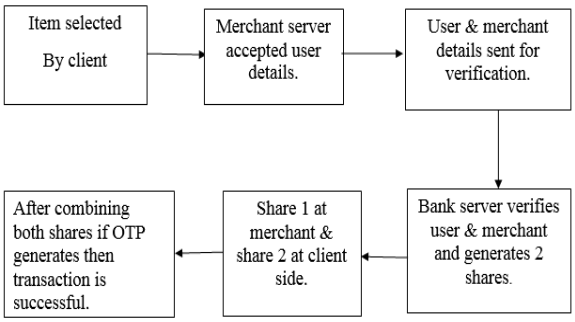

Figure 2. Merchant and bank server

The above figure illustrates what is the role of merchant server and bank server in whole transaction. The user side first log in into the merchant site then it will select the desired product. User information such as user id, user name, password etc. Will send to the merchant server then along with user details merchant details also send to the bank server for verification such as merchant server id, merchant server name, password etc. Bank server plays a vital role in this transaction. It will provide two ways authentication like it will verify both user and merchant server.
User has its unique login password and transaction password so if fake user is there then it is also verified by bank server. When user login to the merchant server along with users details merchant details are also sent to the bank server. Here bank will generate an OTP. By using steganography the generated OTP is converted into QR code. Using visual cryptography the QR code is broken down into two shares. Share 1 is sent to merchant server and share 2 is sent to the client via mail.
At client side we provide combine button for combining both the shares. Merchant will provide share 1 to client and share 2 is taken from mail. After combining both the share QR code is generated. After scanning that QR code we get original OTP. Again client will send that OTP to bank server for verification then it will ask for transaction password if the password is correct then the transaction happen.
In case of fake user, the user details are sent to bank for verification so bank will get to know that fake user is there. If fake merchant is there then bank will generate two fake shares. One will give to fake merchant server and second original share to client via mail. But at the time of combining both shares due to one share is fake it will not generate QR code. So OTP is also not generated. This is how two way authentication and is provided.

V.STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY ALGORITHM

Steganography and visual Cryptography are the two methods that we are using in our project. Through this we are making the transaction secure and help in better security. In our project we are using the steganography technique to hide the OTP (generated by bank server) in the QRcode. The visual Cryptography is applied on the QR Code to create the two shares/images of it.

Steganography is the technique of hiding the secret message within other and extraction of secret message at its destination. Steganography takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Visual Cryptography is a special encryption technique to hide the information into images in such a way it be decrypted by the human vision if the correct key image is used.

The aim of our project is to provide the better security during the transaction. Now we need to have focus on the creation of two OTP shares/images through visual cryptography. The process is described in detail below.

Consider the QR code generated from the OTP by steganography technique .In this QR code each pixel have 0 or 1 values of image. We are creating the two shares/images of OTP. For this we using the random matrix of 2-Dimensional.Visual Cryptography uses two transparent images. One image contain random pixels/arrays and the other image contain the secret information or Pixels/arrays. It is impossible to retrieve the secret information from one of the images.

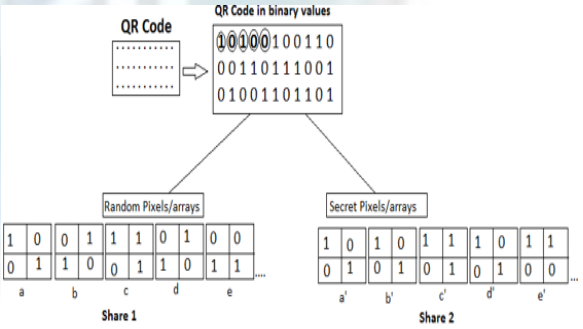

Figure 3. Visual cryptography algorithm

Now while creating the shares we need to do 'XORing' and while combining the shares into one we need to do 'ANDing'. firstly 1st pixel of QR code image (i.e. 0/1 value) XOR with the random generated arrays of 2-Dimensional that is (a) in Random Pixels/arrays with all the pixels/values in that arrays then new matrix is

generated with that is (a′) in Secret Pixels/array. Similarly 2nd, 3rd and so on pixels in the QR code image help in generating the arrays of (b), (c), (d), (e) and so on in the Random pixels/arrays and (b′), (c′) , (d′) , (e′) and so on in Secret Pixels/arrays. If we ANDing of 1st pixel of (a) and 1st pixel of (a′) we can get the original pixel in the QR code. Similarly if we do ANDing of (b) and (b′) and so on. We can retrieve the original pixels of the QR code. This implies that generated images/arrays are the correct keys.

Finally all the arrays of 2*2 matrix in the Random pixels and Secret pixels are collected and merge separately in order to get the complete share 1 and share 2. The share 1 is in random array and which is sent to the merchant server (in request and response form). The share 2 is in Secret arrays and which is sent to be Client by mail.

VI.PROPOSED PAYMENT METHOD

In the proposed solution, we are authenticating the client as well as merchant server. So the information of customer which is given to the bank side and merchant side is the issue of security. The system helps to clients to prevent phishing by providing authentication of merchant. This it is a secure system. This is achieved by the introduction of combined application of steganography and visual cryptography. In this process, shares are created by bank server and they are given to client and merchant server. First share is given to merchant server and another share is given to client via mail. After receiving both the shares, at client side, they are merged and original QR is obtained. The received QR is verified with the original QR at bank side. Thus authentication of both client and merchant is done.

The system provides well security as compared to previous system. Considering the advantages of the system, it is definitely said that it is better secure system. The process carried is done step by step. So the system is scenario oriented and flow based. Steganography and visual cryptography are the security providing techniques.

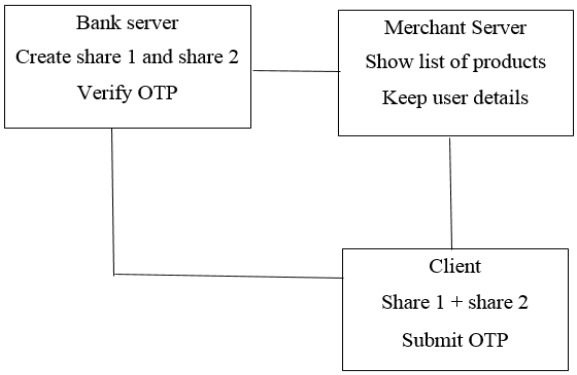

Figure 4. Proposed Payment Method

Figure .a Figure. b

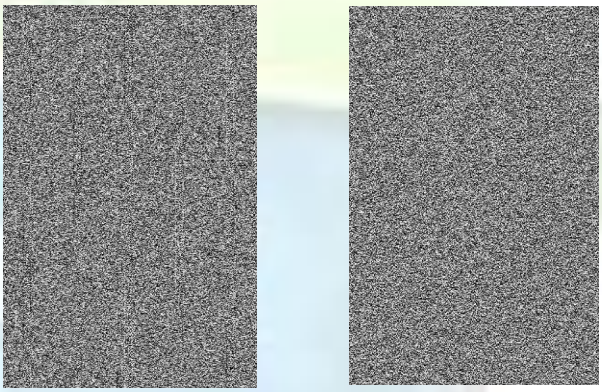

Figure 5. Generated shares

VII. ADVANTEGES

1. The proposed system provides two ways authencation.
2. It also prevents phishing.
3. It uses visual cryptography to create two shares of OTP to make system more secure.
4. The system prevents identity theft.
5. It also provides security to the user personal data.

VIII. CONCULSION

In this paper, two methods are used such as Steganography and visual Cryptography to provide secure transaction during online shopping. It secure the customer confidential information as well as merchant credential and prevent misuse of data at bank side by Admin Application. . This method is mainly concerned with preventing identity theft and providing customer data security. It also prevents phishing. The system authenticates client as well as merchant server (i.e. two authencation).

REFERENCES

[1] Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceeding of IEEE Students' Conference on Electrical, Electronics and Computer Science , Jadavpur University, Kolkata-700032, India, 2014.

[2] Thiyagarajan, P. Venkatesan, V.P. Aghila, G. "Anti-Phishing Technique using Automated Challenge Response Method", in Proceedings of IEEE-International Conference on Communications and Computational Intelligence, 2010.

[3] N. Chou, R. Ledesma, Y. Teraguchi, and D. Boneh, "Client-side defense against web-based identity theft," in Proc. 11th Annu. Netw. Distribut. Syst. Secure. Symp, San Diego, CA, Feb. 2005.

[4]Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3,n 4, October/December 2006.

[5] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994.

ABOUT AUTHORS

Priyanka Tanaji More

Pursuing B.E. degree in (Computer Engineering),Savitribai Phule Pune University, NBN SinhgadSchool of Engineering, Ambegaon (Bk), Pune 411041, India.

Pooja Kantaprasad Tiwari

Pursuing B.E. degree in (Computer Engineering), Savitribai Phule Pune University, NBN Sinhgad School of Engineering, Ambegaon (Bk), Pune 411041, India.

LeenaShriKrishna Waingankar

Pursuing B.E. degree in (Computer Engineering), Savitribai Phule Pune University, NBN Sinhgad School of Engineering, Ambegaon (Bk), Pune 411041, India.

Vivek Kumar

Pursuing B.E. degree in (Computer Engineering), Savitribai Phule Pune University, NBN Sinhgad School of Engineering, Ambegaon (Bk), Pune 411041, India.

Asst. Professor Avinash M. Bagul

Has received masters (M.Tech) Degree From Dr. B. A. Technological University,Lonere in 2012. He is working as Asst. Professor in Computer Engineering Department of NBN Sinhgad School of Engineering Ambegaon (BK), Pune. He is Having 5 years of experience. His area of Interest is computer Networks, Data Structure and Algorithm.

