ISSN 2395-1621

Robust and Secure Online Payment System Using Steganography

[#1]Rhutuja Jain, [#2]Namrata Jagtap, [#3]Surabhi Bhagat, [#4]Sonal Angre

[1]rhutujajain30896@gmail.com,
[2]namratajagtap941@gmail.com,
[3]surabhibhagat95@gmail.com,
[4]sonalangre1597@gmail.com

[#1234]Department of Computer Engineering
TSSM's, BSCOER, Narhe, Pune.

ABSTRACT

The rapid development of data transfer through internet has made it easier to send the data accurately and faster to the desired destination. There are many transmission media to transfer the data to the destination like e-mails, social sites etc. At the same time it is may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are many approaches like cryptography and steganography. Online payment systems allow fund transfer with the help of internet. Nowadays, credit cards are used commonly for payment on e-commerce. There has been a tremendous growth and attraction towards the online shopping in recent time throughout the world. But on the other side we have a major task in hand to protect personal as well as banking information. After the rapid use of online transactions the rise in debit & credit card fraud and steeling the personal information is the real worry for the end users and online retailers. This paper studies the existing approaches for providing limited information which is necessary for fund transfer thereby safeguarding customer data and preventing identity theft.

Keywords: E-Commerce, Information Security, OTP, Steganography, Visual Cryptography, Identity Theft, Phishing.

ARTICLE INFO

Article History

Received: 1st December 2017

Received in revised form :

1st December 2017

Accepted: 4th December 2017

Published online :

4th December 2017

I. 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. 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, 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.

In 2017, news was published which told that OTP was hacked by the white-hat hacker.

Online shopping uses internet, network and web -based technologies in creating interactive medium between sellers and customers. In addition, the existence of online shopping yield benefits such as easy to business transaction network; saves times and reduces search costs compared to conventional shopping process. Because of these benefits, businesses and companies are increasing their use to business transaction through fetching method of delivery using online shopping. With the recent growth of online shopping, it has become an attractive option for expanding the business opportunity available for sellers .Steganography is a technique or a method of hiding the information into the image. It is the practice of concealing a file, message or image into another file, message or image. Steganography combines the word steganos and graphein. The meaning of steganos is covered or protected, the meaning of graphein is writing. The

message which is hidden may be in invisible link between the visible lines of personal letter.The advantage of this technique is that the hidden message does not pay attention to itself as an object scrutiny. It includes hiding of information within computer files. For the transmission purpose media files are considered as ideal because of their large size. Electronic communication involves steganography coding within transport layer.

Cryptography is the practice and the study of techniques for secure communication in the presence of arbitrator. It is special encryption technique in which visual information is encrypted in such a way that decryption does not require a computer.

The method proposed in the system 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 prevents misuse of information at merchant side. In this system there are two shares of image which are combined to get original image. In this way the system provides secure transaction.

II. PROBLEM STATEMENT

In a core banking system, there is a shot of experiencing fashioned mark for exchange. In the net saving money framework, the secret key of client might be hacked and abused. In this manner Security is still a test in these applications. Here, we propose a procedure to secure the client data and to keep the conceivable fraud of marks and secret word hacking.

III. LITERATURE REVIEW

In [1] Sneha M. Shelke, Prof. Prachi A. Joshi , "A Study of Prevention of Phishing Threats using Visual Cryptography", 2016, proposed method preserves personal information of users. In this paper, anti phishing solution based on visual cryptography has been presented. Using proposed method, end user can easily identify the website is real or fake based on validation of image captcha. Additional security is provided by using OTP. This method provides additional security in terms of not letting the invader log-in into the account even when he knows the mail or id of a particular user.

In [2] N. Shrivastava1, T. Verma, "A Survey on Various Techniques for Generating Image Steganography with Improved Efficiency", 2015, in proposed method the sender is hiding the information which is to send to the beneficiary as pictures. The picture is a blend of the content which is gotten from the two procedures of the content steganography which has been inferred before. The two procedures utilized are Reflection Symmetry and the Vedic Numeric technique. The sender sends the information into apportioned shape or we can say that the information which is sent by the sender is divided into 2 sections and separate-isolate part is sent to the two procedures. We are doing this as though the Vedic strategy it,which requires more memory. In this way, the content in the wake of being prepared by the two procedures is combined to shape an entire content and after that the content is changed over into picture by the different techniques or calculations ex. LSB, network augmentation. In this way, the content is changed over into picture that is sent to the recipient.

In [3] S. Roy, P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", 2014, new strategy is proposed, based steganography and visual cryptography, which minimizes data sharing to the merchant however empower effective store exchange from customer's record to vendor's record subsequently shielding purchaser data and avoiding abuse of data at dealer side. The strategy implemented specially for Ecommerce.

In [4] Rahna E, V. Govindan, "A Novel Technique For Secure, Lossless Steganography With Unlimited Payload And Without Exchange Of Stegoimage", 2013, proposes a novel procedure which tries to understand all the above issues in steganography. In the proposed strategy, rather than substitutions we are utilizing the idea of matches between personal information and cover picture. What's more, we additionally utilize the idea of altered recurrence for every character in English. The proposed technique is lossless, has limitless payload limit, has key size which is just around 10 to 20 rate of the message estimate and has more security.

In [5]P. Vaman, C. Manjunath, Sandeep , "Integration of Steganography and Visual Cryptography for Authenticity", 2013, proposes a procedure using picture utilizing Steganography and visual cryptography, and afterward partitioning it into shares. The picture extensions can be .jpg or .png. The message process is computed utilizing the MD5 calculation and this is affixed with the message. The annexed message is then encoded utilizing the AES calculation. The mystery enters utilized as a part of the AES calculation is scrambled utilizing the RSA calculation. The affixed scrambled message is inserted in the picture utilizing the minimum huge piece calculation. The encoded picture is transmitted. The secret word must be given before transmitting the picture document. At the beneficiaries side the watermarked picture record is taken as the information. The message in the picture record is removed utilizing the LSB calculation. The removed message is separated into the process and the message part. The message process is figured for the message and is contrasted and the got one. In the event that they are similar then message is said to be verified.

IV.PROPOSED SYSTEM

In the proposed solution, we are authenticating the client as the information of customer which is given to the bank and the merchant is the major issue of security. The system helps the clients to prevent phishing by providing secure transaction. This is achieved by the introduction of combined application of steganography and visual cryptography. In the proposed system, client shares the secret image to the merchant side. Then merchant splits the

encrypted image into two parts and shares half encrypted image to client and the other half image remains to the merchant itself, after that both the splitted images are combined to verify the authorized user. In this way the system provides secure transaction during the money transferring from one account to another.

V. ALGORITHM

- **Blowfish Algorithm**

The proposed system uses the Blowfish algorithm. The algorithm is used to encrypt the data file. This algorithm is a 64-bit block cipher with a variable length key. Blowfish algorithm requires less amount of memory. It uses only simple operations and also it is easy to implement. It is a 64 bit block cipher ,hence a fast algorithm to encrypt the data. It requires 32 bit microprocessor at a rate of one byte for every 26 clock cycles.

VI. METHODOLOGY

- **Image Uploading**

In this approach, image uploading is must for creating the secret image for hiding the information for security purpose. Firstly system have to add packages for accessing the methods and functions. Then it adds the drives for connecting the database. After that it creates the connection link for database. Then system put the proper sql query for storing the image into database.

- **Mail sending**

Here merchant system sends the mail using the API (javax.mail) to client, where client needs a SMTP (Simple Mail Transfer Protocol) server.

- **OTP generation**

Here OTP in a typical two-factor authentication application, user authentication proceeds as follows: a user enters username and password into a website or other server, generates a one-time password for the server using OTP running locally on a smartphone or other device, and types that password into the server as well. The server then also runs OTP to verify the entered one-time password.

VII. ADVANTAGES

1. The proposed system provides three- way authencation.
2. It also prevents phishing.
3. It uses steganography and visual cryptography to create two shares of image to make system more secure.
4. The system prevents identity theft.
5. It also provides security to the user's personal data.

VIII. CONCLUSION

In this paper, we use visual Cryptography to provide secure transaction in online shopping. It secures the customer's confidential information as well as merchant's credentials and prevents 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 attacks.

IX. ACKNOWLEDGEMENT

We wish to express our profound thanks to all who helped us directly or indirectly in making this paper. Finally We wish to thank to all our friends and well-wishers who supported us in completing this paper successfully. We are especially grateful to our guide Prof. M.K.Mokashi for his valuable guidance. Without the full support and encouragement of our guide, the paper would not have been completed on time.

REFRENCES

[1] Sneha M. Shelke, Prof. Prachi A. Joshi ,A Study of Prevention of Phishing Threats using Visual Cryptography,2016.

[2] N. Shrivastava1, T. Verma, "A Survey on Various Techniques for Generating Image Steganography with Improved Efficiency", International Journal of Advanced Research in Computer Engineering & Technology , vol. 4, no. 3, pp. 1005-1009, March 2015.

[3] S. Roy, P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", IEEE Conference on Electrical, Electronics and Computer Science, vol. 6, no. 2, pp. 88-93, 2014.

[4] Rahna E, V. Govindan, "A Novel Technique For Secure, Lossless Steganography With Unlimited Payload And Without Exchange Of Stegoimage", International Journal of Advances in Engineering & Technology, vol. 6, no. 3, pp. 1263-1270, July 2013.

[5] P. Vaman, C. Manjunath, Sandeep , "Integration of Steganography and Visual Cryptography for Authenticity", International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 6, pp. 80-84, June 2013.

