New Approach to Online Payment System
Himanshu Joshi1 Mohit Patil2 Mohmmad Jakir3 Charushila Talekar4
1,2,3,4 Department of Computer Engineering
Trinity College of Engineering and Research Pune, India

Abstract—It has been observed lately that a massive amount of crowd is diverting itself to the most efficient platform i.e. the e-commerce market for personal online shopping. During this process debit cards, credit cards and internet banking facility is regularly used for any purchase of product. This elements involve a lot of confidential data which are necessary to complete the payment but also has many intrusion risks. To avoid this data stealing, to improve the internet security and increase confidentiality of data this method is proposed which uses visual cryptography and steganography to function efficiently.

Key words: Data Confidentiality, Phishing, Visual Cryptography, Steganography

I. INTRODUCTION

Online shopping involves usage of debit and credit cards which has highly confidential data and if the data is stolen by unauthenticated user it could result in a massive indentity theft and unvalidated fund transfer. This misuse of personal information can lead to mistrust in internet security and loss of users in huge numbers. The process of Phishing is an illegitimate action that involves stealing of personal user information to steal personal identity and make unvalidated financial frauds. In this paper, a new platform is been proposed , that uses steganography and visual cryptography which absolutely demolishes any chances of sharing information with the online merchant but successfully fund transfer from consumer’s account to merchant’s account therefore keeping safe the user information and avoid misuse of that information from the merchant side. This mechanism could also be extended beyond online shopping level as it could be used in physical banking.

BPCS-Steganography is process of hiding textual confidential data in the image which is 24 bit color image and the process involves removing confidential data and the image after removing this complex areas is very large.

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. This two above mentioned techniques are used in detail for well-planned and coherent functioning of the proposed method.

II. PREVIOUS WORK

A brief survey of previous related work in the field of internet banking security based on cryptography and steganography is presented in this section. Various customer authentication systems using visual cryptography are presented before but it is only used for physical banking. A signature based authentication and validation system was proposed previously but even this platform also requires the physical presence of the customer. Another proposal was based on visual cryptography and steganography authentication system for customer authentication in internet core banking. A textual message authentication image algorithm was proposed to protect against e-banking fraud. A biometrics with respect to visual cryptography is used as an efficient authentication system.

Another proposal based on text steganography uses characteristics and alphabets of English language like mandatory word order, inflexion and use of periphrases for data hiding process and avoiding the usage of properties of a sentence. This gives flexibility and sense of freedom from the perception of ability of construction of sentences and also increases computational complexity which has to be avoided.

The steganography technique is based on an ancient vedic numeric code in which coding is based on tongue position. Every letter is assigned or nominated a number in range of 0 to 15. This ancient cryptographic technique has been used for encrypting the data which happens to be very confidential or for communication between two individuals. For different frequencies, different numbers are assigned to the letters. It means that it is representing frequency of letters in integer form. This encryption technique has been efficiently used in the past as it is hard for an intruder to decrypt the message represented using this technique.

III. SYSTEM DESIGN

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

IV. PROPOSED METHODOLOGY AND RESULT

In the proposed system, consumer will submit to information to merchant’s site which will further verify by central Certified Authority (CA). This is done by the central Certified Authority (CA) and combined application of visual cryptographic and Steganography technique. Validation of receipt of payment from authentic consumer is done by information obtain by merchant. It can be in form of card and account number related to the card which is used for shopping. The following sequence will gives a complete idea:

- Step 1: Registration process of Consumer.
- Step 2: generation of Share 1 using Visual Cryptography and Steganography
- Step 3: opts for online shopping (Merchant Side) by consumer.
- Step 4: completion of shopping process and directed to payment process.
- Step 5: submission of share 1 provided during registration and Merchant provides its account details.
- Step 6: Combination of Consumer Share and Bank Share and verification by the CA.
- Step 7: Validation of share stipulates synchronization to bank.
- Step 8: For valid share, Bank will extract the Account number from the original image afterwards it will perform transaction.
- Step 9: Consumer will be notify by mail.

**VII. FUTURE SCOPE**

The payment system could be expanded to be implemented for physical banking. As this method believes in preventing identity theft and misuse of confidential user data so it could also be used in small business which has a customer base as purchase in the stores can also be done with the use of credit and debit cards for which the security has to be ensured.

This can also be implemented for standardization of a particular product or a community by making their personal identification or confidential identity secured and make it remain confidential.

**REFERENCES**