Secure Transaction Scheme using encryption and steganography based on secure image Cryptographic Primitives

#1 Abhijeet Lokhande, #2 Sanket Gujar, #3 Gunjan Patil

1 lokhandeabhijeet11187@gmail.com
2 sanketgujar50@gmail.com
3 gunjanpatil999@gmail.com

Department of Computer Engineering
JSPM’s, JSCOE Pune.

ABSTRACT

We present a new approach for providing limited information only that is necessary for fund transfer during online shopping thereby shielding customer data and increasing customer confidence and preventing identity theft. The system combined using Steganography and visual cryptography for providing more secure. In the project proposed solution, 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 is achieved by the introduction of combined application of steganography and visual cryptography. In this project we use two shares of OTP which are combined to get original OTP. In this way the system provides secure transaction. Here also use the secret image during the money transferring one account to another.

Keywords: E-Commerce, identity theft, steganography, visual cryptography.

I. INTRODUCTION

Online shopping is the retrieval of product information via the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier. Identity theft and phishing are the common dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misusing 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. Phishing is an illegitimate 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 focused industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption inhibits the interference 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. In this paper, a new method is proposed, that encompasses both steganography and visual cryptography, which minimizes detailed information sharing between consumer and online merchant but enable successful fund transfer from consumer’s account to merchant’s account thereby safeguarding consumer information and preventing misuse of information at merchant’s side. The method proposed is applied to E-Commerce but can be easily extensible for other applications like online banking.

ProjectObjective:
The main motive of the proposed system prescribed in this paper is to handle applications that require a high level of security, such as E-Commerce applications, core banking and internet banking. This can be done by using combination of two applications: Steganography and Visual Cryptography for safe online shopping and consumer satisfaction. Online shopping is generally considered as retrieval of product information via the Internet and issue of...
purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier. Identity theft are the common dangers of online shopping. Identity theft is the stealing of someone’s identity in the form of personal information and misuse of that information for making purchase and opening of bank accounts or arranging credit cards.

II. LITERATURE SURVEY

“Online Payment System using Steganography and Visual Cryptography”, In this paper steganography and visual cryptography used. 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. [1]

“Anti-Phishing Working Group (APWG), “Phishing Activity Trends Report”, APWG has re-instated the tracking and reporting of unique phishing reports (e-mail campaigns) in addition to unique phishing sites. An e-mail campaign is a unique e-mail sent out to multiple users, directing them to a specific phishing web site (multiple campaigns may point to the same web site). APWG counts unique phishing report e-mails as those in a given month with the same subject line in the e-mail. [2]

“The security of shopping online” Online shopping, personal information security is a major problem in the Internet. Summarizes the characteristics of online shopping and the current development of the main safety problems, and make online shopping related security measures and transactions. [3]

“The emperor’s new security indicators: An evaluation of website authentication and the effect of role playing on usability studies” He evaluate website authentication measures that are designed to protect users from man-in-the-middle, ” phishing”, and other site forgery attacks. he asked 67 bank customers to conduct common online banking tasks. Each time they logged in, we presented increasingly alarming clues that their connection was insecure. [4]

“Hiding Information in Document Images”, Spatial information to reliably hide data in document images. Experimental results reveal that this information survives the distortions introduced by noisy image reproduction devices. [5]

III. PROPOSED DESIGN

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing least 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 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.

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

System Architecture:

Modules:
Our system has mainly three modules, an administration module, an authorized user module, and other user module. Various processes involved in these three modules are:

User Module:
User can authorize login access. He can update all personal details. He also can's authority to generated secure encryption process.

**Upload Image:**
User uploaded image while account creation. That image is encrypted and splits for share the image to further process.

**Money Transfer:**
While Transfer money another account then secure encrypted image must to upload.

**Admin Module:**
Admin is the authorized person, he check all the user activity records as well as profile.

### IV. ALGORITHM

In this paper we use the following algorithm for implementing the secure system.

1. **Blowfish Algorithm**

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

2. **Image Uploading Algorithm**

   In this project image uploading is must for creating the secret image for hiding the information for security purpose. Firstly you have to add packages for accessing the methods and functions. Then you have added the drives for connecting the database. Then you create the connection link for database. Then you put the proper sql query for storing the image into database.

3. **Mail sending algorithm**

   Here we send the mail using the API (javax.mail). You need a SMTP (Simple Mail Transfer Protocol) server.

4. **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.

### V. CONCLUSION

In this paper, we use 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.

### REFRENCES


