ISSN 2395-1621

Advanced Secure Online Payment System Using Stegano Image

[#1]Sneha Ghawate, [#2]Sanika Gaikwad, [#3]Archana Tate, [#4]Rasika Joshi

[1]ghawatesneha.22@gmail.com,
[2]sanikagaikwad1996@gmail.com,
[3]archanatate9823@gmail.com,
[4]joshirasika151@gmail.com

[#1234]Department of Computer Engineering,

MMCOE, Karvenagar, Pune-411052

ABSTRACT

This paper presents a new approach for providing limited information only that is necessary for fund transfer during online shopping there by shielding customer data and increasing customer confidence and preventing identity theft. The system combined using Steganography and cryptography for providing more secure. The proposed solution is 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 cryptography. This paper 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 from one account to another.

ARTICLE INFO

Article History

Received: 10th December 2017

Received in revised form :

10th December 2017

Accepted: 14th December 2017

Published online :

14th December 2017

Keywords: E-commerce, Identity theft, Steganography, 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 i n 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 48days 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 methodology is proposed, that can provide more security, we combine steganography and cryptography, which remove more detailed information sharing between consumer and online merchant but activate 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 proposed system is applied to online shopping otherwise E -commerce but can be easily extensible for other applications like online banking.

Overview

The main objective of the proposed system is to handle applications that require a high level of security, such as E-Commerce applications, core banking and internet banking. This can be proposed by using combination of two applications:

Steganography and Cryptography for secure online shopping and consumer satisfaction with privacy. Online shopping is mostly considered as fetching of product information via the Internet and issue of purchase order through online shopping using debit/credit cards 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. PROPOSED SOLUTION

We have created system in java. Data is stored in mysql database. We have created a web application with local server. Web application that communicates with local server and Trustee Server using REST API. We have uploaded image for hiding the data on database. We have evaluated time required for tag generation and image encryption checking for authorized valid person.

In the proposed system, information which is submitted by the consumer to the online website at merchant's site is minimized by providing only minimum information. It will only verify the payment made by the consumer from its account.

This is accomplished by the introduction of a central Certified Authority (CA) and combined application of visual cryptographic Steganography and technique. The information which is obtained by the merchant will only validate receipt of payment from authentic consumer. It can be in the form of account number related to the card used for shopping.

III. LITERATURE SURVEY

The problems more associated with online shopping, the consumer's protection in most important during the transaction that requires privacy and trust between different geographical locations or countries [1]. There is increasing threads over online shopping because of insecurity, lack of customer's protection and trust which are vital elements for a successful online transaction between customer to customer, organization as well as individual.

In [2], report we analysis major problem faced by people in an online transaction or shopping is security. From survey report, it is widely happening transaction base on e -commerce have been constrained by security. In addition he analysis, consumers are concern about their privacy when their personal information are required to facilitate transaction besides, potential risks are also posed to those using credit cards to make purchase online. Secured system with privacy is needed to enhance online shopping since consumers cares for their privacy and security. Furthermore, [2] online shopping paves way to fraudulent act and unworthy credit orders which is also attributed to unsecured services. Trust also plays an essential role on consumer's choice for online purchase.

Roca et.al. [3] explain that trust in online businesses environment determines consumers' willingness to engage in online business area. He used security such as the use of digital signature and certificates could be more secure in controlling or avoiding risk of fraud for online-based transactions [3].

In another study [4], it was pointed out that sec urity, protection policy and as well as reliabilities of companies are major barriers to online shopping. However, consumer's behavior towards online shopping includes and not limited to [5]; concern over unauthorized sharing of personal information, unsolicited contacts from the online retailer, and undisclosed tracking of shopping behavior. Besides, system security-consumers who are concern about illegal bridging technological protected devices to acquire consumer's personal, financial or transaction -related information. Concern over online retailer fraud cause by purposeful misrepresentation or non-delivery of goods paid for are among the potential threat over online purchase.

Improved security system for online shopping could reduce unworthy behavior of consumers' with increase intention for online transaction [6]. Disposing of the customer's personal detail and credit card information during and after online transaction should be avoided as it gives more room for illegal use of customer's information. Trust in online transaction could be enhanced through policies that incorporate legal, technical, rigorous standards for security, data protection and as well as certificates of independent trusted third parties [6].

Improved security in online shopping could tremendously encourage consumers to engage in e -commerce deal as well as its awareness and role among Libyan economic units. Consumers feel relaxed to use online medium when their capital and information are properly protected [7].

In addition, online sellers should encourage trustworthy relationship in order to increase and attract consumers to online transaction by ensuring that every transaction is kept within the scope of agreement [8]. Owing to the need to facilitate e-commerce transaction in Libya we hereby proposed that efficient measures for effective implementation of e -commerce transaction in Libya economic developments should integrate web -based infrastructures.

IV. ALGORITHMS USED

1. Encryption algorithm.

Encryption is the process of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers. The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a priva te key by which a recipient can decrypt the message.

2. Blowfish Algorithm

The subkeys are calculated using the Blowfish algorithm:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P -array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64 -bit key, then AA, AAA, etc., are equivalent keys.)

3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).

4. Replace P1 and P2 with the output of step (3).

5. Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.

6. Replace P3 and P4 with the output of step (5).

7. Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

RSA

RSA (Rivest–Shamir–Adleman) is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem". The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1978. Clifford Cocks, an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in

1973, but this was not declassified until 1997.[1], A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with cur rently published methods, and if the public key is large enough, only someone with knowledge of the prime numbers can decode the message feasibly.[2] Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem remains an open question.. RSA is a relatively slow algorithm, and because of this, it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key, which is what we use to encrypt our message, and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break.

3. Image Uploading Algorithm using RSA

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.

4. Mail sending algorithm

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

Email is emerging as the one of the most valuable service in internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.

SMTP Fundamentals

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

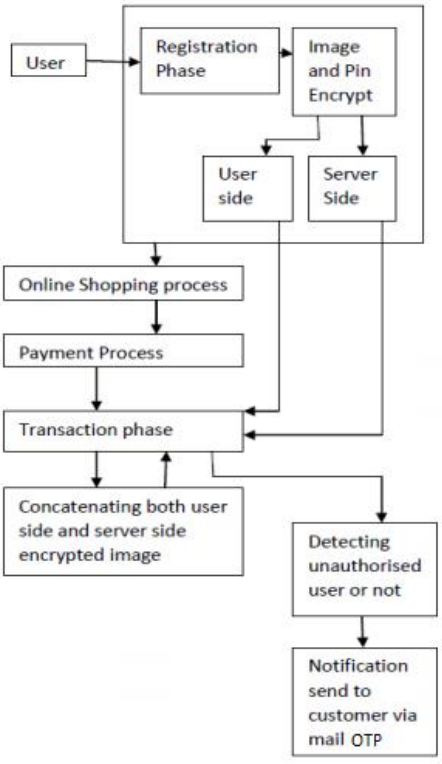

Fig. 2. System architecture

It is tested for online or offline video. It does not require any expensive or dedicated software. A webcam is the only device required. The system output detects the information about th e eye state either it open or close which can be applied in many applications like: eye typing, detection of driver fatigue etc.

V. CONCLUSIONS/FUTURE WORK

In this paper, we use encryption technique to provide secure transaction during online transaction. It secures 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.

REFERENCES

[1] Patton M.A., Josang A., "Technologies for Trust in vol. 4, pp. 9 -21, 2004.

[2] Udo G.J., "Privacy and Security Concerns As Major Barriers for E -commerce: A Survey Study," Information Management & Computer Security, vol. 9, no.4, pp.165-174, 2001.

[3] Roca J.C., Garcia JJ., de la Vega JJ., "The Importance of Perceived Trust, Security and Privacy in Online Trading Systems," Information Management & Computer Security, vol. 17, no. 2, pp. 96-113, 2009.

[4] Chen Y-H., Barnes S., "Initial Trust and Online buyer behavior," Industrial Management & Data Systems, vol. 107, no. 1, pp. 21-36, 2007.

[5] Roman S., Cuestas P.J., "The Perceptions of Consumers Regarding Online Retailers' Ethics and Their Relationship with Consumers'General Internet Expertise and Word of Mouth: A Preliminary Analysis," Journal of Business Ethics, vol. 83, pp. 641–656, 2008.

[6] Grabner-Kraeuter S., "The Role of Consumers' Trust in Online-Shopping" Journal of Business Ethics, vol. 39, pp. 43-50, 2002.

[7] Salo J., Karjaluoto H., "A Conceptual Model of Trust in the Online Environment" Online Information Review, vol. 31, no.5, pp. 604-621, 2007.

[8] Mukherjee A., Nath P., "Role of Electronic Trust in Online Retailing" European Journal of Marketi ng, vol. 41, no. 9/10, pp. 1173-1202, 2007.

[9] Hunaiti Z., Masa'deh R.M.T., "Electronic Commerce Adoption Barriers in Small and Medium -Sized Enterprises (SMEs) in Developing Countries: The Case of Libya" Ibima Business Review, no. 2, pp. 37 -43, 2009.

