ISSN 2395-1621

Secure Online Payment System using Encryption and Steganography Technology to avoid Phishing Attack

[#1]Priyal Kharate, [#2]Prof. Deepti Varshney

[1]priyalp.patil@gmail.com

[#12]Department of Computer Engineering
Shree Ramchandra College of Engineering, Wagholi, Pune.

ABSTRACT

We 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 visual cryptography for providing more secure. In the project proposed solution, are authenticating the client as well as merchant server. Here we send 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 OTP for security purposed. In this way the system provides secure transaction. Here also use the secret image during the money transferring one account to another.

ARTICLE INFO

Article History

Received: 12th March 2018

Received in revised form :

12th March 2018

Accepted: 15th March 2018

Published online :

15th March 2018

Index term: Phishing attack, 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 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 visual 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.

Project Objective:

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 Visual 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. REVIEW OF LITERATURE

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 security, 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.

III. SYSTEM OVERVIEW

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.

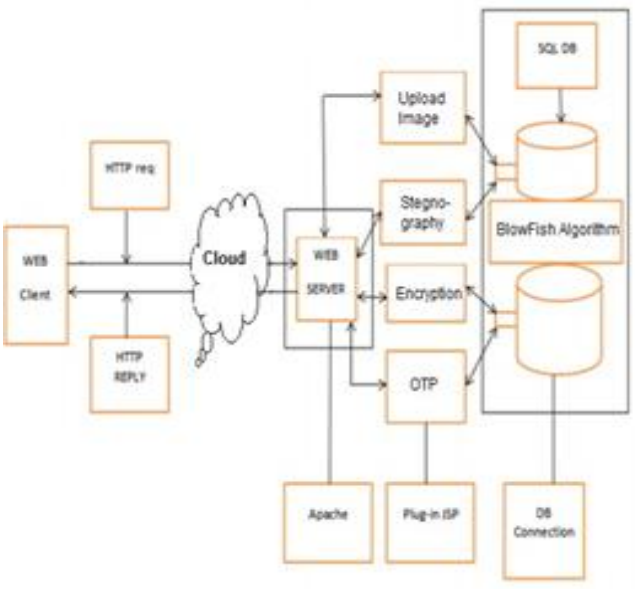

Fig 1. System architecture

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 cans 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. SYSTEM ANALYSIS

We implement these system for avoiding the network security threads occurring when people online transaction. We analysis this system using the following points: In this paper we use the following algorithm for implementing the secure system.

1. Blowfish Algorithm

In this paper we proposed the Blowfish encryption algorithm to encrypt the data file. This algorithm is more secure rather than other encryption algorithm. Blowfish 64-bit block cipher with a variable length key. This algorithm mostly used because it operation process requires less memory. It uses only simple processing steps, therefore it is easy to implement. It is 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. SOFTWARE REQUIREMENT SPECIFICATION

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 on cloud. We have evaluated time required for steganography and encryption process generation. Here we also check online transaction details of each user.

VI. MATHEMATICAL MODEL

Our system can be represented as a set

System S = {I, O, C, ES}

Where,

I=set of inputs
O=set of outputs
C = set of constraints
ES= Encryption and Steganography

I=Input:
Input I = {U,E,S,D}
Where,
U : Upload image on DB.
E : Encryption function call. S : Steganography.
D : Decryption O=Output:

Output O = {E,P,N}
E=Encryption done,
P=Payment successfully transfer,
N=notification

C=Constraint
C = {C1, C2}

Where,
C1 = "User should enter a query related to any data".
C2 = "Client Machine and server should always be connected.". Encryption data will store database.

Response Time: The system shall give responses in 5 second.

User-interface: The user-interface screen shall respond within 5 seconds.

VII.EXPERIMENTAL ANALYSIS

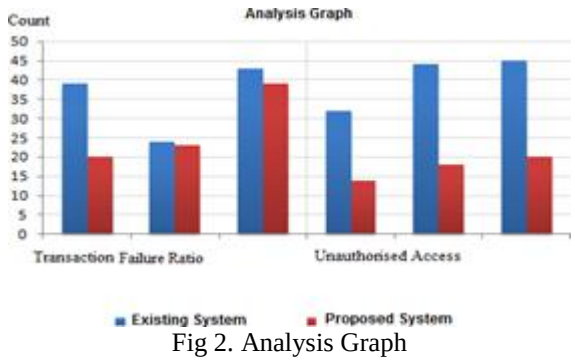

Fig 2. Analysis Graph

VIII. CONCLUSION

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.

IX. ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well- wishers who supported us in completing this paper successfully I am especially grateful to our guide Prof. Deepti Varshney madam for him time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] Abdulghader.A. Ahmed, Hadya.S.Hawedi Online Shopping and the Transaction Protection in E- Commerce: A case Of Online Purchasing,2012.

[2] C. Vanmathi, S. Prabu A Survey of State of the Art techniques of Steganography,2013.

[3] Joel Lee, Lujo Bauer, Studying the Effectiveness of Security Images in Internet Banking,2014.

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

[5] Souvik Roy and P. Venkateswaran, Online Payment System using Steganography and Visual Cryptography,2014.

[6] Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shopping online," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011.

[7] Hu ShengDun, U. KinTak, "A Novel Video Steganography Based on Non-uniform Rectangular Partition," Proceding of 14th International Conference on Computational Science and Engineering, pp. 57-61, Dalian, Liaoning, 2011.

[8] S.Premkumar, A.E.Narayanan, "New Visual Steganography Scheme for Secure Banking Application," Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 – 1016, Kumaracoil, India, 2012.

