ISSN 2395-1621

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

[#1]Prof.V.B.Khedekar, [#2]Gujar Sanket, [#3]Lokhande Abhijeet, [#4]Patil Gunjan

[1]vilaskhedekar2010@gmail.com
[2]sanketgujar50@gmail.com
[3]lokhandeabhijeet11187@gmail.com
[4]gunjanjpatil999@gmail.com

[#1234]Department of Computer Engineering
JSPM'S, Pune.

ABSTRACT

In this paper we present a new technology for online transaction system. We providing limited information only, as compare to other application. User providing information that is necessary for fund transfer during online shopping there by shielding customer data and increasing customer confidence and preventing unauthorized access network and get catch the sensitive data. The system combined using Steganography and visual cryptography for providing more secure. In the proposed solution model, are providing the client as well as merchant server security. Here we send information of customer which is given to the bank side and merchant side is the issue of security. The proposed system provides better security to clients to prevent phishing by providing authentication of merchant. This system is design by the introduction of combined application of steganography and visual cryptography using the blowfish algorithm. In this project we also maintain duel security level for advance security using OTP(One Time Password) 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.

Index term: Encryption, network attack, Blowfish algorithm, steganography, OTP.

ARTICLE INFO

Article History

Received: 14th May 2019

Received in revised form :

14th May 2019

Accepted: 16th May 2019

Published online :

17th May 2019

I. INTRODUCTION

Today's User is mostly used online shopping website for purchasing the any product for personal use and make payment online for that product.Once user payment for that product then user filling of credit or debit card information and shipping of product by mail order or home delivery by courier. Here user don't know that online payment portal is secure or not? Then Identity theft and phishing are the most common dangers attack happen during payment transferring for 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 customer data are mostly loss and information was misused as a result of identity theft. Anti-Phishing is a mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. The Payment application, Financial Service are the most focused and wieldy used industrial sectors also attack happen of phishing attacks. Secure Socket Layer (SSL) encryption inhibits the interference of consumer information in transit between the consumer and the online merchant. In this proposed solution, a new methodology is introduced, that can provide more security, we combine steganography and image encryption, which remove more detailed information sharing between consumer and online merchant output of the system is 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 work of the proposed system is to provide applications that require a high level of security to the E-Commerce applications, core banking and internet banking.

Main objective can be proposed by using combination of two techniques: 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

In [1] the problems are more increases with online shopping and online payment, the customer protection is most important during the online transaction that wants privacy andtrust between different geographical locations or countries [1]. There is increasingattacks and threadsover online shopping or online payment because of insecurity,un-authorization access 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 he analysis and review major problem faced by customer in an online transaction or shopping is security. From survey report, it is mostly 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] the author explain 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.

In this paper the author [3] explain that trust is most important in online businesses environment determines consumer's willingness to engage in online business area. He implements security such as the use of digital signature and certificates are mostly used and more secure in controlling or avoidingrisk of fraud for online-based transactions [3].

In another study [4], explain the e-commerce for goods services during online transaction. Itwas 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 miss-behavior of consumers' with increase intention for online transaction [6].Here user 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. Once information get then attacker misuse that information for other purpose. 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].

In this study author improved security in online shopping could widely use and 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 portal is encourage trustworthy relationship between customer and online portal 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 isminimized by providing only minimum information. It will only verify the payment made by the consumer from itsaccount. This is accomplished by the introduction of a central Certified Authority (CA) and combined application ofvisual cryptographic Steganography and technique. The information which is obtained by the merchant will only validatereceipt of payment from authentic consumer. It can be in the form of account number related to the card used for shopping.

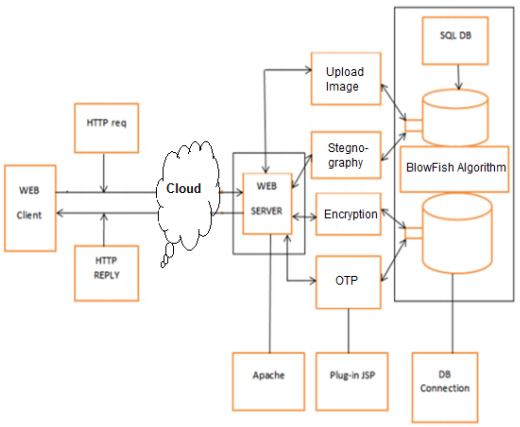

Fig 1. System architecture

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 system we implement the blowfish encryption algorithm to encrypt the providing information during the online payment. This algorithm is more secure rather than other encryption algorithm. Blowfish 64-bit block cipher with a variable length key. This algorithm is widely used because it operation process requires less memory and more secure. It uses only simple processing steps, therefore it is easy to implement. Itis fast algorithm process to encrypt the given customer 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 (One time password) in a typical two-factor authentication application, user authentication proceeds as follows: User authentication purposed we used the OTP as login phase, once authentication success then we used another OTP during online payment transfer.

V. SOFTWARE REQUIREMENT SPECIFICATION

We have created system in java technology. Data is stored in mysql database. We have created a web technology application using JSP with local server. Web application that communicates with local server and Trustee Server using REST API. We have uploaded image on local cloud. We have evaluated time required for steganography and encryption processgeneration. Here we also check online transaction details of each user.

VI. MATHEMATICAL MODEL

System Description:

Input:

- Upload image ()
- U : Upload image on DB.
- E : Encryption File.
- S : Steganography.
- D : Decryption.

Output:

- Encryption data will stored database.

Input:

- Function check (id, request, image)
- ID: unique id for each image.
- Request: User request for image.
- Image: Image check both side server and client.

Output:

- Amount will transfer to another person.

Success Conditions: Our system success when secure image is valid for transaction.

Failure Conditions: Our system fails when no any security policy apply to the image file.

VIII. RESULT

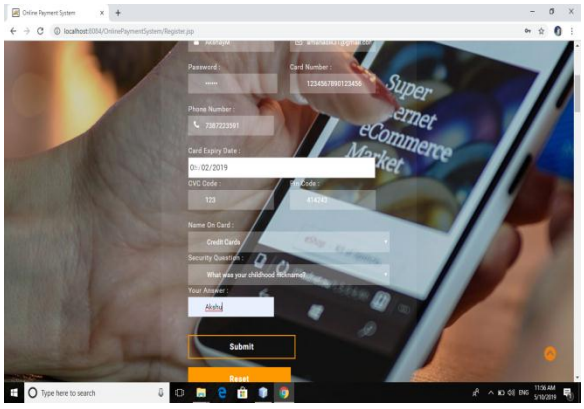

Fig 2. Registration page

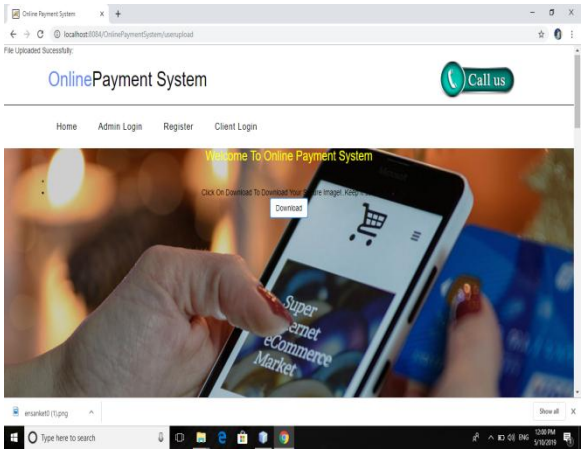

Fig 3. Secure image

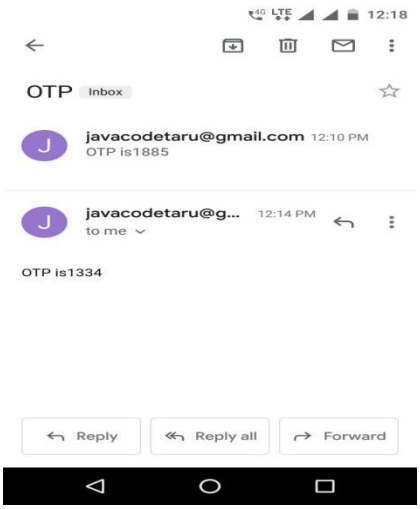

Fig 4. OTP notification on mail

IX. CONCLUSION

In this research paper, we use encryption technique using blowfish algorithm and steganography to hiding the data to provide secure transaction during online transaction. It secures the customer confidential information as well as merchant credential and prevents misuse of data at bank side by Admin Application. This technique is mainly implementing with preventing identity theft, providing customer data and also prevents phishing.

X. 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.V.B.Khedekar 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, XiaoyaoXie, 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.

