OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SECURE ONLINE PAYMENT SYSTEM USING ENCRYPTION AND STEGANOGRAPHY TECHNOLOGY TO AVOID PHISHING ATTACK

Priyal PrakashKharate[1], Prof. Deepti Varshney[2]

Department of Computer Engineering,Shree Ramchandra College Of Engineering, Lonikand, Pune, India
priyalp.patil@gmail.com[1], varshney.deepti11@gmail.com[2]

Abstract: **In this paper we propose a revised paradigm for Secure Online Payment System. We provide limited information required for transaction, as compare to other application. User avail information required for payment transactions during for online shopping thereby protecting sensitive data of customer and maintaining reliability, also preventing unauthorized access to network and get catch the sensitive data. The system combined using Steganography and visual cryptography for providing more secure. The proposed solution model not only provides client security but also merchant server security. In the current system, we provide customer information to the merchant side and bank side which compromises security. The proposed model provides better security to clients that avoid phishing attack by providing authentication of merchant. This system is designed by the introducing two new technologies steganography and visual cryptography which are combined together in the application and using the blowfish algorithm. In this paper we also maintain duel security level for advance security using OTP (One Time Password) for security purposed. Thus, the system provides secure transaction. Here we also use the secret image during the transaction from one account to another**

Keywords: Phishing attack, identity theft, steganography, visual cryptography

---∴∴∴---

I INTRODUCTION

Today's user mostly uses online shopping website for purchasing the any product for personal use and make payment online for that product. During the purchase of the product user fills in credit or debit card information for the payment and then the product is shipped for home delivery by courier or mail order. In this case, user is not aware of online payment portal, if it is secure or not? This results to identity theft and phishing, the two are the most common dangers of online shopping encountered during online payment system. Identity theft is stealing of personal information of the user and misusing the stolen information in different ways, either for purchase of products or services, it can also be used for opening bank accounts. Even credit cards can be falsely created while misusing the information. Anti-Phishing on the other hand is a mechanism that employs both social engineering and technical assets to prevent stealing consumers personal information and financial account details. When it comes to payment systems, financial services are the most prone in industrial sectors for phishing attacks. Secure Socket Layer (SSL) encryption inhibits the interference of user information while the transaction between the buyer and the online seller takes place. In this proposed solution, a proposed methodology is introduced, that can provide more security, where we combines teganography and image encryption, which removes sensitive information sharing between user and online seller. The output of the system proposes successful payment between consumers account to merchants account thereby securing customer information and safeguarding misuse of information at merchants side. The proposed payment system is applicable to online shopping and E-commerce sectors and can be easily extended for different transaction systems like online banking.

Project Objective:

The main work of the proposed system is providing systems that ensures more security to the E-Commerce and payment applications, core banking applications and internet banking facilities. The objective of the proposed system is achieved by involving two valuable techniques: steganography together with visual Cryptography for secure online shopping and maintaining consumer privacy. Online shopping consists of fetching the product information via Internet through online portals and issue of purchase order through online shopping using debit/credit cards requests, the debit or credit card information is filled by customer followed by shipping of

product by mail order or home delivery by courier. Identity theft that is theft of personal information and phishing are the most common dangers of online shopping. Stealing of someone's personal information and misusing the stolen information for making purchase or creating new bank accounts, arranging credit cards etc.

II REVIEW OFLITERATURE

The [1] problems increase in online shopping and payment as the customer's data protection is most important for online transactions that requires privacy and ensures trust between distinct geographical areas [1]. Increasing attacks and threats over online purchase or online payment due to insecure, un-authorization access and lack of customers security and belief are important aspects for a successful online transactions for any system or individual.

In this we review major issues faced by customer's in online transaction. From survey report, it is mostly targeted transaction for online shopping sites have been constrained by security as online systems are easy targets to attack. In addition, the analysis also involves consumers who are concerned about the security of their personal information is required. Besides, the risks are also for those who are using credit cards to make purchase online. The secured system are required now that ensures safety and privacy to data. Furthermore, [2] the author explain online shopping creates a way to fraudulent act and unworthy credit orders which is also part of unsecured services for online payment. Trust and reliability are also important factors on consumers choice for online purchase.

In this paper the author [3] explain that trust is most important in online e-commerce environment as it determines customers preparedness to involve in the online transaction system. Digital certificates and signature are commonly used in controlling or avoiding risk of fraud and for providing security of online-based transactions[3].

In other study [4], author explains the e-commerce for goods and services during online transaction. It was observed that protection policies that ensures security and re-liability over companies providing services are the barriers to online shopping services. However, consumers responses towards online purchase includes [5] ;concer over sharing of sensitive personal information, unsolicited contacts from the online shopping system, and tracking of shopping activities. Besides system security, consumers are also concerned about illegal bridging devices that are technologically protected to acquire consumers personal, financial or transaction related personal information. Concern is also raised for information sharing with online payment retailers, fraud that is caused by purposeful non-delivery of goods already paid for which is among the potential threat over online shopping.

Improved security model for online purchase could minimize customer's miss-behavior with introducing intent for online transaction [6]. Disposing of the customers banking details, and card details during and after the online transaction should be avoided as it is prone to illegal use and miss-use of the customers information. Once information get then attacker misuse that information for other purpose. Putting trusting.

Online payment system could be improved by introducing policies that are technically sound, incorporate legal, rigorous standards for security of data or information and with the issue of certificate so find dependent trusted third parties[6].

In this study author enhanced security of online shopping system could widely use and consumers are encouraged to engage in online shopping or e-commerce as well as creating awareness and role among Libyan economic units. Consumers feel confident and relaxed while using online medium if their capital and personal information are properly protected and secured [7].

In addition, online portal should include elements that encourage trustworthy relationship between customer and online portal in order to improve the purchase of goods and to attract customers to online transaction. The portals should also ensure that every transaction is based and fulfills the agreement [8]. The protection of the customer data and security brings awareness and trust in Libiyan economic units. Customer's thereby feel confident and secure while transacting online.

III SYSTEMOVERVIEW

In the newly proposed system, the sensitive data of the customer is submitted for online payment with online portals at merchants website is reduced by providing only minimum and necessary information which is secured. The only data verified in this process is the payment made by the consumer. This is accomplished by introducing the central Certified Authority (CA) and a payment system of visual cryptography and Steganography techniques together. The information sent to the merchant side is only validate receipt of payment made by the authentic consumer. It can be either in the form of account number that is related to the card used for shopping.

Modules

The system is based on three modules, an administration module, an authorized user module, and other user module. The different 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.

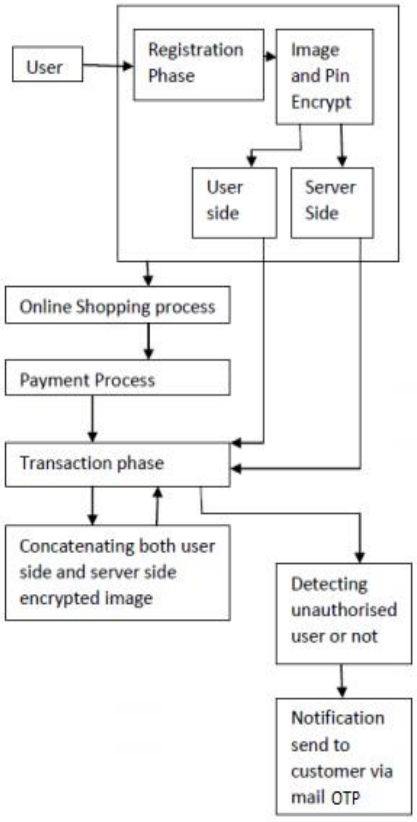

Figure 1. System Architecture

IV SYSTEMANALYSIS

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 is a 64-bit block cipher text with a variable length key. This algorithm is widely used for the operation as the process requires less memory and more security. Simple processing steps are involved, therefore it is easy to implement. It is fast algorithm process to encrypt the given customer data. It requires a 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

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 process generation. Here we also check online transaction details of each user.

VI MATHEMATICAL MODEL

System Description:

Input:

- Upload image()
- U:UploadimageonDB
- 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 trans-action.

Failure Conditions:

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

VII EXPERIMENTAL ANALYSIS AND RESULT

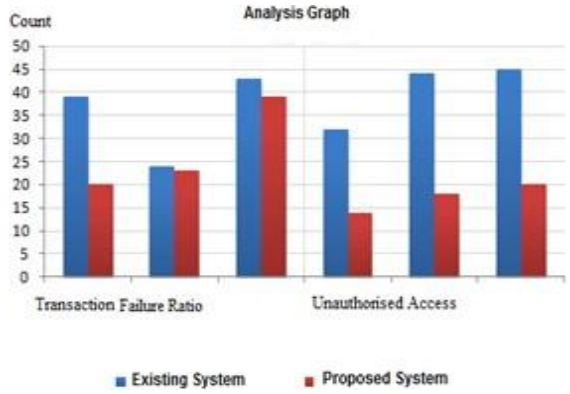

Figure 2. Analysis Graph

The above analysis graph shows the ratio of transaction failures in proposed as well as existing system. The graph clearly shows the higher probabilities of successful transactions as compared to existing system.

Moreover, the unauthorized access monitored in the existing system is much higher than the proposed system. In the proposed system it can be minimized by more than 50%.

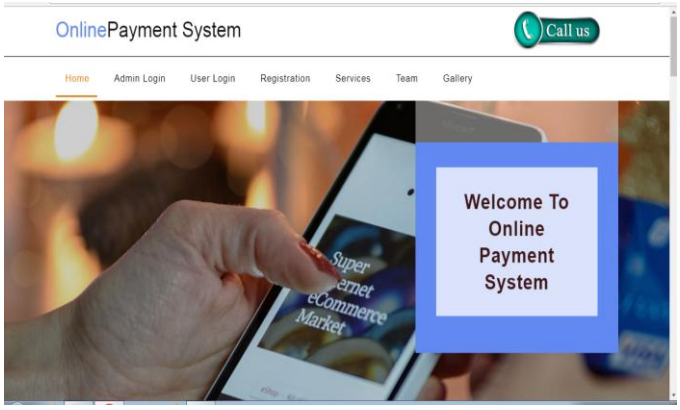

Figure 3. Online Payment System

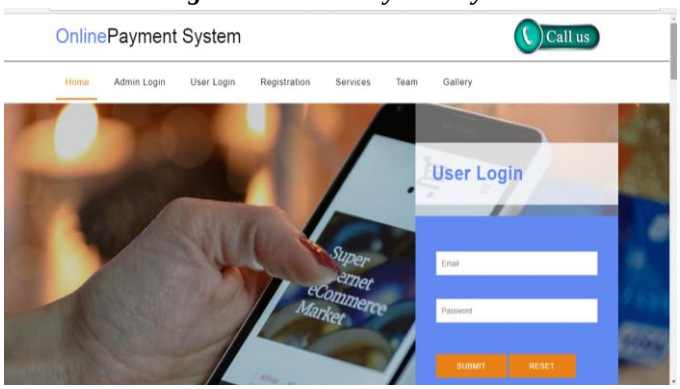

Figure 4. User Login

Figure 5. Registration Form

ACKNOWLEDGMENT

It gives us immense pleasure in presenting the research paper for our project ”Secure Online Payment System Using Encryption and Steganography Technology to Avoid Phisihing Attcak”. I would like to thank and appreciate Head Of Department Prof. Deepti Varshney for the efforts put by her in the project and the valuable guidance. I am also thankful to all the staff member of Department of Computer Engineering, Shree Ramchandra College of Engineering, Pune for providing all the necessary facilities which were indispensable in the completion of this paper, support, comments, suggestion and persuasion

REFERENCES

[1] Abdulghader.A. Ahmed, Hadya.S.Hawedi Online Shopping and the Transaction Protection in E-Commerce: A case Of Online Purchas- ing,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 InternetBanking,2014.

[4] Sneha M. Shelke, Prof. Prachi A. Joshi , A Study of Prevention of PhishingThreatsusingVisualCryptography,2016

[5] Souvik Roy and P. Venkateswaran, Online Payment System using Steganography and VisualCryptography,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 Con- ference 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 Confer- ence on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 1016, Kumaracoil, India,2012.