Online Payment System with Phishing and DDOS Detection and Prevention

Mr. Swarjit Suryawanshi
UG Student
Department of Information Technology

Mr. Dnyaneshwar Mule
UG Student
Department of Information Technology

Ms. Kavita Chemate
UG Student
Department of Information Technology

Ms. Priyanka Jadhav
UG Student
Department of Information Technology

Mr. Gajanan Arsalwad
Assistant Professor
Department of Information Technology

Abstract

Security is the one of most important feature of banking sector. E-commerce safety is the one of the uppermost visible security that controls the end user during their day to day life and payment interaction with their business. Sharing of account related data in insecure medium raises security and privacy issues. Personal sensitive data can be theft by hackers. So it is need of today's E – commerce world for providing the solution of that problem and helps to increase the confidence of customer for making the use of digitalization. This proposed system provides secure payment system which helps for move toward for the result of economic business deal transaction. It is helpful for reducing scam by providing only that information which is necessary for the fund transfer and provides the security against various security threats.

Keywords: Cryptography, Detection, E-commerce, Prevention, Phishing, Security, Steganography etc

I. INTRODUCTION

Identity theft is the robbery of someone's identity in the form of private data and doing misuse of that data for doing the transaction or any illegal activity like arranging credit or debit cards. In 2012 user information was misused so much for purpose of stealing identity [1]. Phishing is an unlawful mechanism that employs both communal and technological deception to steal consumer's private identity information and economic account transactions [8]. In 2nd quarter of 2013, Payment Service, economic and wholesale services are the most targeted industrial sectors of phishing attacks [14]. To avoid such type of attack on transaction or E-commerce sector is very much important. This proposed system will fulfill the user's requirement and helps to increase the trust relationship between user, merchant and E-commerce sector.

A. Purpose:

The purpose of this system is to provide the security to user private data in the online transaction by providing the two way security protection that is making use of text steganography and visual cryptography and to provide the detection and prevention of DDOS attack and detection and prevention of phished websites and webpage.

B. Scope of Project:

This software system will be strong secure payment system for online transaction of fund by applying two way security mechanisms with detection and prevention of phished website. This system will be designed for minimizing the sharing of user sensitive data between user and seller for achieving the prevention of fraud of stealing user sensitive data.

II. SYSTEM ARCHITECTURE

The online payment system has four active components that are customer, seller, bank, CA which will interact with each other for processing the online transaction securely. Customer will purchase some item from online shopping portal and add it to cart and for making its payment he will direct to payment system and the customer will enter his payment detail according to payment type that is debit card and credit card. After that payment system will apply security mechanism on that user data for secure transmission of data through public network and produce share and send it to certified authority then CA will send one share to customer and keep one share for himself after receiving the share user will provide his share to CA and seller will provide his account detail to CA then CA will combine those share for achieving customer bank details and those shares to bank after that bank will verify decode that shares and reveal user info and verify that detail and make transfer of fund to seller

account after that generate notification message for seller and customer and send it to both on their mail or register mobile number**.**

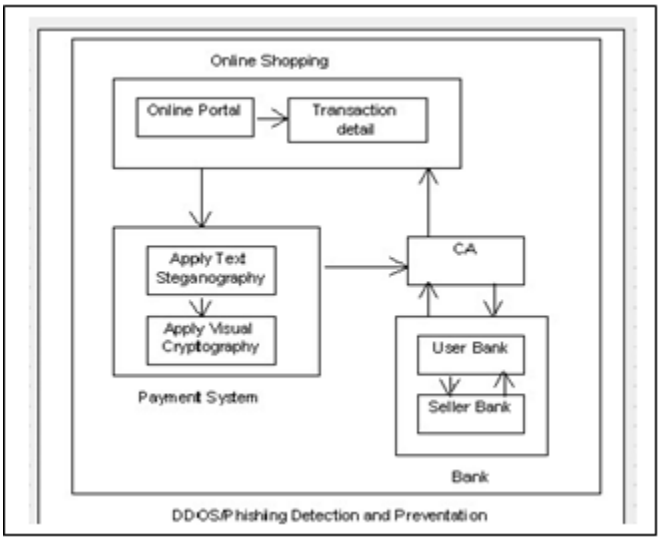

Fig. 1: System Architecture

III. MODULES

A. Customer and Bank Registration:

In this module user firstly register to web site after registration user will make login into the system to get complete access of e-commerce application. This module also contains the bank registration. Admin also register to the new bank to our e-commerce application for transaction purpose.

B. Shopping or Item Selection:

After login to system client/user can browse shopping portal for selection of items. After choosing of items user will send payment order to e-payment server after filling essential fields. But that data can be theft by the fraud person so security of sensitive data is most important. Shopping activities are carried out in following way. While shopping user will visit the online portal and register himself and login to the merchant site and then search the item after that he will select the item according to his wish and add that selected item into cart and select the payment option. Then user will get directed to the payment system for making further transaction. Then user will add the transaction details and further transaction will get place.

C. Secret Key Generation:

1) Steganography:

It is the procedure of masking the user confidential data in another media or files. In steganography we can use different media file as a covered media. But in this system we are using the text for hiding the user data. Texts are masked without leaving any sign of existence of secret data in cover media [3]. In text steganography cover text is called as stego cover which is used to conceal the user data. And sensitive data is called as embedded text. Cover text will remain same after hiding the user text. It enhances the complexity and embedding size of stegocover. According to survey of steganography algorithm text steganography is mostly preferable as compared to other steganography algorithm [5]. The structure of text documents is identical with original text, while in other media such as in picture, the structure of document isget changed from original data. Text requires a less memory to process and store and it is easy to communicate.

2) Visual Cryptography:

It is the encryption scheme used for concealing the user sensitive information in image and splitting that stego image in different shares [11]. It creates two shares images one contains random [empty] pixel and other contains sensitive information. Fundamentally it is kind of secret sharing mechanism and it protect the data very strongly as compare to other security mechanism because first thing it hiding the secret data in image without leaving any sign on it and again it is dividing that data in two shares images, So third party is not able to reveal the original content of the data until and unless those both shares combine together [9].

a) Encryption Algorithm

Input: Shares and covering images

Output: Embedded image

Method: **Procedure Stamping (shares, cover images)**

1) Measure the collection of pixel colours for shares, cover images and secret image coordinate (x, y).
2) Compute amount of pixels in share's black and white region of secret image.

3) Compute the number of data pixels overlapped at coordinate (x, y).
4) Set the indicator for coordinate to 0 i.e.., available for stamping cover pixel.
5) Add cover pixels on selected coordinates (x, y) of shares. The data pixels will be added on candidate coordinate (x, y) of share that has empty pixel on it.
6) Loop Steps 3 to 5 until all require cover pixels are printed on shares.

b) Recover Image

Extract the hidden secret images and secret shares. By arranging the shares in correct order will get an original secret image is done using the algorithm. At the destination they arrange the shares by using the logical or operation and extract an original secret image. The attractiveness of this is that set of qualified participants is able to extract the content of secret image.

Input: Embedded images

Output: Secret image

1) Reveal the data in covering images and the shares from the imprinted images.
2) Overlie the shares in the specific order with legal password.
3) Original content of the overlapped image will be retrieved.
4) In case the order gets change or fetching of wrong secret key.

D. Transaction in Online Shopping:

1) Encoding:

In this process, Steganography uses various aspects of English language like inflexion, order of permanent word and use of passage for concealing information rather than pretty using properties of a certainty. This gives manipulation of sentence construction and it increases computational complexity.

Input: Text file

Output: secret key image shares

2) Decoding:

Input: Two secret key images/shares

Output: Original secret key image

Customer verification detail is transfer to the seller by certified authority. Ahead obtaining client verification phrase known only to a restricted group, bank matches it with its database records and after satisfying authorized client, transfer fund from the client/node record to the stated merchants account.

E. Linkguard Algorithm for Phishin :

Link guard algorithm is used for prevention and detection of phishing attack which works by comparing the visual link and the actual link. It also evaluates the similarities of a URI with known trusted sites. Following are the steps used in link guard algorithm [14].

1) Define variables used in algorithm
   Vi_link = visual link;
   Ac_link = actual link;
   Vi_dns = visual DNS name;
   Ai_dns = actual DNS name;
   Sender_dns = sender's DNS name.
2) Retrieve the visual and actual DNS value
   Vi_dns = GetDNSName (Vi_link);
   Ac_dns = GetDNSName (Ac_link);
3) Compare the visual and actual links
   if Vi_dns and Ac_dns are not empty and Vi_dns! = Ac_dns
   Then return PHISHING;
   If Actual_dns is dotted decimal then
   Return POSSIBLE_PHISHING;
4) Compare encoded links
   if actual link or visual link is encoded then
   Vi_link2 = decode (Vi_link);
   Ai_link2 = decode (Ai_link);
   Goto Step 3;
5) Evaluate the name of domain for possible phishing
   If (Vi_dns is NULL)
   Goto step 6;
6) Analyze the actual DNS name according to the blacklist and white list.
   if actual dns is in blacklist then
   Return PHISHING;

if actual dns is in whitelist then
Return NOTPHISHING;
Goto Step 7;

7) Match the pattern
If Sender_dns and Ac_dns are different then
Return POSSIBLE PHISHING;
For each item Previ_dns in seed-set
Bv = Similarity (previ_dns , actual-link);
If bv == true then
Return POSSIBLE_PHISHING;
Or return NO_PHISHING;

8) Check the similarity
If str is part of actual-link
Return true;

9) Evaluate the maxlenght and minchanges
if thresh < (maxlen-minchange)/maxlen< l then
Return true;
Return false;

F. Detection and Prevention of DDOS:

Dos attack is going to become a more popular and more frequent scheme to acquire web pages/sites and web servers down. This attack is simple to do and so much difficult to providing the security against this type of attack, that's why they are so popular. To avoid ddos attack we can block the response to the attackers. We haven't control over the requests, so we need to catch the attacker as early as possible afterwards request received by web server [16].

Following are two challenges to block the attacks.

1) Recognize the attackers.
2) Block the response simply to the recognized attackers.

To discover the attack as early as possible, an http module is a best. It is executed at the starting of any page or handler as a result of that module it can reduce the load on the server. This http module checks all received requests and block that request which is coming from those IP addresses that make lots of requests in a short time span. The module gives the high performance and lightweight security from dos attacks and very easy to execute.

IV. FUTURE SCOPE

In comparison to other banking application which uses Steganography and visual cryptography are basically used for physical banking, the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

V. CONCLUSION

In this paper, we developed a payment system for online transaction by combining various methods such as steganography and cryptography that provides customer data security, privacy and it prevents misuse of data by third party. This system explains the recognition of identity theft and customer data security and discovery and avoidance of phishing webpages/sites using linkguard algorithm.

REFERENCES

[1] Souvik Roy and P.Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science,2014
[2] R Chandramouli and N. Memon, "Analysis of LSB Based Image Steganography Techniques", Proceeding of the 2001 International Conference on Processing, vol.3, pp. 1019-1022, 2001
[3] Jaya, Siddhartha Malik, AbhinavAggarwal and Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011
[4] ChetanaHegde, S. Manu, P. DeepaShenoy, K. R. Venugopal and L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications," Proceedings of 16th International Conference on Advanced Computing and Communications, pp. 65-72, Chennai, India, 2008
[5] S.Premkumar and 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
[6] MoniNaor and Adi Shamir, "Visual Cryptography", EUROCRPT1994. [http ://www. fe.infn. it/u/ filimanto /scienza/webkrypto/visualdecryption.pdf]
[7] Pranita P. Khairnar and Prof. V. S. Ubale, "Steganography Using BPCS technology, "in Proc. International Journal Of Engineering And Science , May 2013. Vol.3(Issue 2),pp 08-16.International Journal of Engineering Research & Technology (IJERT)ISSN: 2278-01
[8] U.Naresh, U.VidyaSagar and C.V. MadhusudanReddy, "Intelligent Phishing Website Detection and Prevention System by Using Lin Guard Algorithm," in Proc. IOSR, 2013. Vol. 14(Issue 3), pp 28-36
[9] ChetanaHegde, Manu S, P DeepaShenoy, Venugopal K R and L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,", in Proc. 16th IEEE International Conference on Advanced Computing and Communications,2008

[10] 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
[11] 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
[12] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu,"Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos.3 & 4, pp. 313- 336, 1996
[13] Yang Jing "On-line Payment and Security of E-commerce". ISBN 978-952-5726-00-8 , 2009 International Symposium on Web Information Systems and Applications (WISA'09)
[14] PhishGuard.com. Protect Against Internet Phishing Scams.shttp://www.phishguard.com/
[15] The Anti-phishing working group. http://www.antiphishing.org/
[16] V.Priyadarshini, K.Kuppusamy,"Prevention of DDOS attack using new cracking algorithm" ,IJERA,vol.2,issue 3,may-june 2012,pp.2263- 2267.