ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 3, Issue 4 , April 2016

Advance Phishing Detection Using Visual Cryptography And One Time Password

Prof N.R.Jain ,Kashid Ujwal , Shaikh Apsara, Patel Nikhil, Divekar Tejashri

Department of Informaion &Technology Engineering, PDEA'S College Of Engineering , Hadapsar,Pune, Maharashtra, India

ABSTRACT: Advance Phishing Detection Using visual cryptography and OTP system aims at providing the facility to detect whether the site is phishing or not and will solve the problem of identity theft and phishing attack .Phishing is an act in which a user's credentials is stolen such as username, password, credit card details etc for malicious reasons . In this system both the merchant and the client are registered to the bank and both are authenticated by the bank server. The OTP is obtained at the client end only when the client and the merchant put their shares. OTP is verified by the bank server and if the OTP is valid the merchant server is detected anti phishing.

KEYWORDS: Phishing, One Time Password(OTP), Visual Cryptography, Shares, Authenticate.

I. INTRODUCTION

Now a days people are at large using e-commerce sites in which most of the bank related transactions occur which increases the threat of losing all bank /card details. In these types of transactions we are not aware of that whether it is valid card holder or someone else is using other's card for the purpose of stealing or theft. Also there are lots of different fake sites which look similar as that of original sites due to which normal person who don't know much about internet and fake sites are easily trapped with these sites and might lose all their bank details and other personal details.[1] Hence such practices will enhance the phishing in the internet world. There are lots of incidents in the real world where such activity have taken place and victims have survived empty handed. Many freely available antiphishing browser extensions tools that warns user when they are browsing a suspected phishing sites .due to its demerits need of effective technique is needed.[2]To curb this, lots of anti-phishing technique[3] [4][5][6] have been invented and implemented in recent past. But we are developing such a unique system in which we intend to protect the users from the phishing attacks which is "Advance Phishing Detection Using Visual Cryptography and OTP". In this system, the user can check whether the website he is willing to visit is a genuine website or a phishing website. After knowing these he can securely perform all his task and operations. Here the concept of visual cryptography is used.[7]

II. RELATED WORK

Phishing goal is to acquire or steal the someone else data by using legitimate website for own benefits. Phisher make the phishing web pages which look exactly like the web pages of legitimate web site. Phisher send link of the fake website in spoofed email which is send to the victim on the behalf of recognized companies or organzation trying to make the victim convince and visit the fake web sites.And when the victim submit its personal information to the fake website that information are stolen by the phisher for own benefits.

Researchers propose many mechanism to check the site is geninue or phishing website."An Enchanced Anti-phishing framework based on visual cryptography" [4] is one such mechanism in which randomly generated image is decomposed into two shares.The shares are generated for every new session. The trusted server stores the key which is required for decryption purpose. Original image is revealed at user end only when server under test and user are registered to the trusted server else improper image is obtained when either of them is not registered. The main disadvantage of the this system is that we can't trust any server that is letting us know that is site is safe or unsafe for performing our transaction.

Another mechanism is "A novel Anti-phishing framework based on visual cryptography "[5] is one such mechanism in which there are two phases first is registration phase and second is login phase . In the registration phase image captcha is decomposed into two shares.Share one is kept to the user and another is kept with the server. In the login

phase both will stacked together to produce the image captcha. When the captcha is displayed ,user can check the captcha that is displayed is matches with the captcha that is displayed at the registration phase. From this user can detect weather the site is phishing or not according to image captcha. The main disadvantage of this system is that share may get stolen and only at the time of the registration shares are generated.
There are various method are there to check the site is phishing or not many anti –phishing browser extension are also there but they have there own disadvantages. So a need of a new system is very much needed to overcome theseproblems effectively.

III. VISUAL CRYPTOGRAPHY

Visual Cryptography(VC) is one of the cryptography technique which was firstly proposed by Naor and Shamir.[7] which allows any visual information to be encrypted in such a way that the decryption can be performed by the human visual system neither any computation required. The decryption process eliminates the computation problem. Secret image is revealed by stacking operation means stacking the shares. Visual cryptography is very secure, easy to implement and especially useful for the low computation load requirement.
We can achieve this by accessing one of the following scheme:-

1](k,n)-threshold Visual cryptography scheme-In this scheme the secret image is encrypted to n shares such that when any k number are overlaid will reveal the secret image.
2](n,n)-threshold visual cryptography scheme- In this scheme the secret image is encrypted to n shares such that n shares are overlaid to reveal the secret image.
3] (2,2)threshold visual cryptography scheme-In this scheme the secret image is encrypted to two different shares such that both the shares when overlaid will reveal the secret image.
In past, visual cryptography schemes were applied to only black and white images. First colored visual cryptography scheme was developed by Verheul and Van Tilborg [8]. For a colored visual cryptography scheme with c colors, the pixel expansion m is c× 3. Yang and Laih improved the pixel expansion to c × 2 of Verheul and van tilbong. R.Youmaran et al [9] invented an improved visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme provides improvement in the signal to noise ratio of the camouflage images by producing images with similar quality to the originals.
In visual cryptography types of secret image will either binary, gray level or color image and number of secret images are either single or multiple, shares that are generated are meaningful or meaningless as per depending on the scheme. The performance of visual cryptography depends upon on various measures such as accuracy, contrast, pixel expansion etc.

IV. EXISTING SYSTEM

In the existing system Fig.1, the customer password in connection with bank and the customer authentication information in connection with merchant is used. Password is hidden inside the cover text and on the cover text authentication information is stored. Visual cryptography is applied on the cover text and two shares are formed.

One share is with the customer and other share is with the central authority. During transaction process the merchant will direct the customer to the central authority. In the portal merchant submits its necessary account detail and customer will put his share. After that CA will combine his share with the customer share to form the original image. CA will send merchant account details and cover text to the bank. now the customer authentication information is sent to the merchant by CA .Now the bank will customer authentication password is matches with the bank databases. after verifying it the if it is valid the bank will transfer fund from the customer to the merchant account. after receiving the fund ,the merchant payment system validates the receipt of payment using customer authentication information. Transmit number is also appended with the customer information.

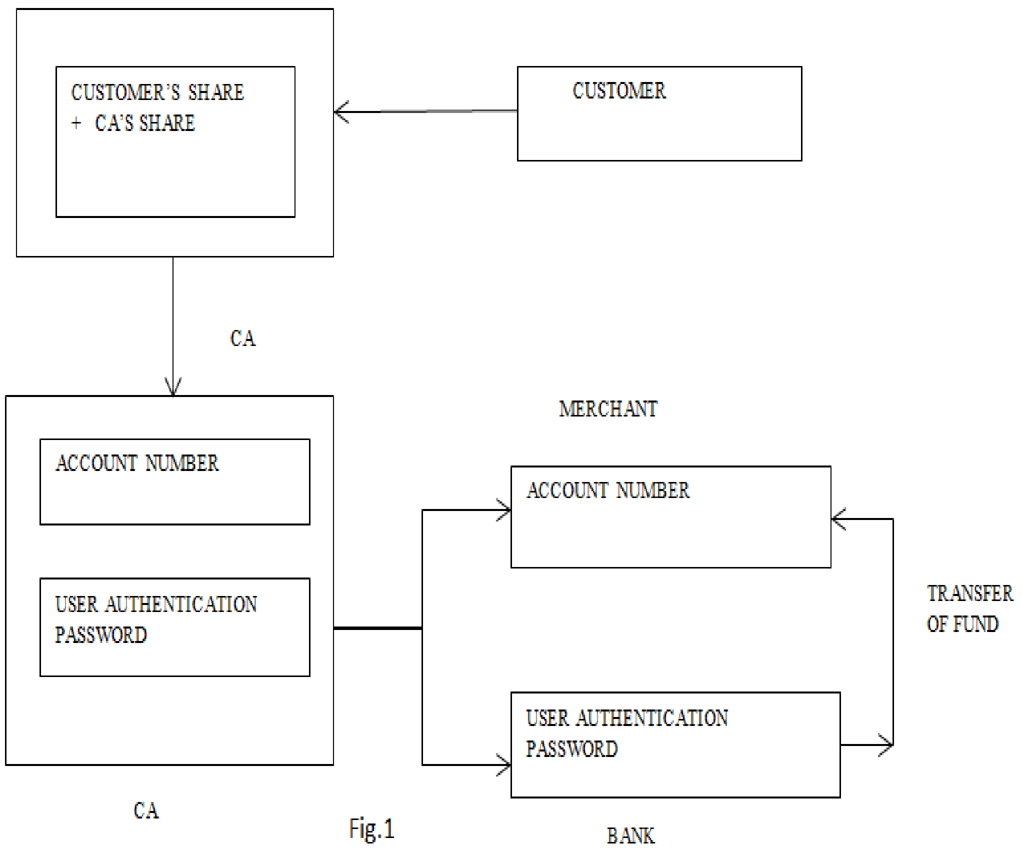

Fig.1

V. DISADVANTAGE OF THE EXISTING SYSTEM

1)Merchant may direct the customer to the portal which is similar as CA portal and get a hold on a customer share this is a major security threat that customer have in the existing system.

2)Password and account no. in connection with bank is used

3) Thrust on 3rd party : Its very difficult to trust someone. Original image is revealed to CA. So CA may misuse the customer information.

VI. PROPOSED SYSTEM

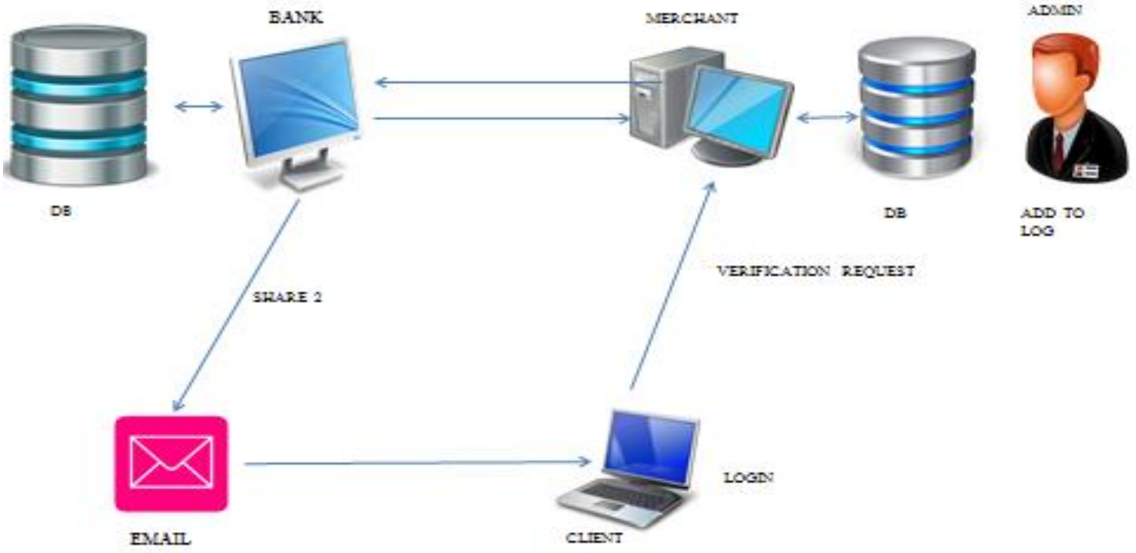

FIG.2 PROPOSED SYSTEM

Proposed methodology :-

For detecting and preventing phishing, we have proposed a new methodology Fig.2 for detection of a phishing website. This will prevent a customer from being one of the victim of the phishing attack.The Proposed framework is shown in above figure. As per our methodology first of all user and the merchant should be registered to the the bank. Once the user is registered to the bank he then can login through the client application using username ,password and url of the merchant sites . The verification request is sent to the merchant server. The merchant will then send its server key,server id ,uid to the bank. Bank will verify the details that is valid or not. If its valid then it will generate otp otherwise garbage will be generated. After that QR will be generated and visual cryptography is applied. Share 1 is sent to the merchant and other share will be sent to the client through email. Merchant and client will put there shares at client application. Both the share combine to give the OTP. If OTP get generated enter the otp for verification the bank server will verify the entered OTP. If the entered OTP is valid then the merchant sites is non phishing otherwise it is phishing. Hence from this method the user can determine the site is safe or not to carry out the transaction.

VII. ADVANTAGE OF THE PROPOSED SYSTEM

1) Authentication :- Client and merchant server are authenticated by the bank serverand OTP is also verified by the bank Server.
2)This system protect the customer from man in middle attack.
3)Security:-customer information is not shared to the merchant until the merchant server is verified .

VIII. CONCLUSION

Now a day phishing is very much common activity. It is a mechanism in which an attacker steals customer's personal identity data and financial account credentials. With our proposed methodology we can easily check whether a merchant site is a genuine website or a phishing website . After knowing these he can securely perform his further proceedings or transactions.

IX. FUTURE SCOPE

In the proposed system many improvement can be done in order to increase its efficiency in the future. The proposed system is a desktop application, so in future we can make android application also. We can use hadoop as a database in future for storing data. Apart from these there is scope for adding more features to it. The proposed system also safeguards our information and prevents middle-man attack. There are many future improvement and future enhancement in the advance phishing detection using Visual cryptography and OTP.

REFERENCES

1]APWG "Phishing Activities Trend Reports 1St quarter 2014.Accessed on 19th July 2014.http://docs.apwg.org/reports/apwg_trends_report_q1 2014.pdf
2]Oinam Bhopen Singhl and Dr Hitesh Tahbildar2 "A Literature Survey On Anti-Phishing Browsers Extension"(IJCSES) Vol.6,August 2015 DOI:10.5121/ijcses.2015.6402 21.
3]Gaurav Madhuresh Mishra Anurag Jain "Anti Phishing Technique :review "International Journal Of Engineering Research and Application (IJERA) ISSN:2278-9622 Vol 2,Issue 2,Mar-Apr2012,pp.350-355 350
4] Gaurav Palande Shekar Jadhav ,Ashutosh Malwade ,Vishal Divekar "An Enhan Phishing Framework Based on Visual Cryptography"ISSN:2278-9359(Volume-3,Issue -3),2014
5]Divya james and Mintu Philip,"A Novel Anti Phishing Framework Based On Visual Cryptography ."(IJDPS) Vol.3,No.1,January2012
6]George Abbound,Jeffrey Marem Roman V.Yampolskiy" Steganography and Visual Cryptography in computer Forensics'IEEE,2010
7]M.Naor, A.Shamir ,in:A.De Santis(Ed.),Visual Cryptography,Advances in Cryptology:Eurpocrypt'94,Lecture Notes in Computer Science,Vol.950,Spriner Berlin,1995,pp 1-12
8] E. Verheul and H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret SharingSchemes." Designs, Codes and Cryptography,11(2),pp.179-196,1997.0
9] R.Youmaran, A. Adler, A. Miri , "An Improved Visual Cryptography Scheme For Secret Hiding", 23rd Biennial Symposium on Communications, pp. 340-343, 2006