IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

Phishing Attack Prevention Using Visual Cryptography

Megha R.Chaudhari[1], Neha D.Chaudhari[2], Shubhangi S.Kanade[3], Sumedh G.Bhadre[4], Dhiraj D.Bhagat[5]

Department of Computer Enginnering, SSBT Collage of Enginnering,Jalgoan,India[1-5]

Abstract: Now days each and every single application which uses security includes authentication process having username and password. Phishing is an effort by an personality or a group to burgle personal con denial in turn such as passwords, credit card information etc from unsuspecting victims for identity theft, monetary gain and other fraudulent activities. Proposed a new approach "Phishing Attack Prevention Using Visual Cryptography" to solve the problem of phishing. Here, an image based conformation, by means of Visual Cryptography (VC) is worn. According to this approach, user registration contains the captcha image as password and the image is splits into two parts using K-N sharing algorithm. For the purpose of user authentication user is sent one share (part of image) and other part of image is on server side. We need to secure Website Authentication process. Here is many approaches present there for cryptographic mechanism but not for website authentication. Though our system has proposed an approach provides authentication of website by using OTP on e-mail id. If OTP is matched then only the login successfully.

Keywords: Phishing attack, image captcha, visual cryptography, OTP.

I. INTRODUCTION

In present days people used to prefer e-commerce, online booking system, online banking system etc. So there are many chances to gain the confidential information by attacker. Attacker can gain the confidential credentials with phishing technique and it is the illegal activity which can perform with different social engineering technique. phishing state that when the attacker uses someones secret in-formation for illegal purpose. Communication channels such as websites, e-mails and to and for e-commerce, online banking instant messaging service is provided by the attacker to stole the secret information of the user. In this case to avoid this type of attack service provider must provide authentication process with user name and password. Phishing is an attempt done by an individual or a group on personal confidential information. So that to avoid this attack image based authentication using visual cryptography is used.

Traditionally, there are many existing approaches based on cryptographic technique but they all suffer from false positive notification. However, proposed approach does not secure from false positive (FP) notification and outperforms all existing approaches. So that in proposed system an image based authentication using visual cryptography (vc)along with dynamic OTP is used. The use of visual cryptography is used to preserve the privacy of image captcha in which the original image captcha is decomposing into two shares that are stored in separate database servers ,so that the original image captcha can be recollect only when both are simultaneously available.

II. LITERATURE SURVEY

'Vimal Kumar and Rakesh Kumar': This paper provides a novel anti-phishing approach based on visual cryptogra-phy. According to this approach a user generates two shares of an image using (2, 2) visual cryptography scheme. Client stores the first share of this image and second share is uploaded to the website at the time of user registration. After this, web-site asks for some other information like second share of the image, username, and password. These credentials of a particular user can change once per login. During each login phase, a user verifies the legitimacy of a website by getting secret information with the help of stacking both shares. There are many existing approaches based on cryptographic technique but they all suffer from False Positive notification. However, proposed approach does not secure from False Positive (FP) notification and out performs all existing approaches .In the future work, proposed scheme is based on centralized approach, centralized server can be problematic when attacker will attack on the server to get the user information. So this problem can be reduced with the help of distributed sever approach.[1]

'**Barnali Gupta Banik and Samir Kumar Bandyopadhyay'**:In this paper a new technique of Image Steganography has been proposed which is using Lorenz Chaotic Encryption to encrypt the secret message, 3 level Discrete Wavelet Transform to hide encrypted data and visual cryptography to share stego image in secret communication. In that paper a new method of steganography has been proposed which is using chaotic encryption to encrypt secret image and visual cryptography for secret sharing of stego image. In this paper author concluded that this is an way of secret sharing in Image Steganography. This method is elective where privacy and security of secret message is much important rather than the quality of retrieved secret message.[2]

'**Divya James and Mintu Philips'**:In that paper they can proposed a new approach named as "A Anti- phishing framework based on visual cryptography "to solve the problem of phishing, Here an image based authentication is done using Visual Cryptography (vc). The use of visual cryptography is used to preserve the privacy of image captcha in which the original image is decomposed into two shares that are stored in separate database servers ,so that the original image captcha can be generated only when both are simultaneously available.[3]

III.VISUAL CRYPTOGRAPHY SCHEMES

A.For Binary Images

Wu and Chen ain 1998 were the first researchers to present the visual cryptography schemes to share 2 secret images in 2 shares. During this scheme 2 secret binary images were thought of that were hidden into 2 random shares, specifically share A and share B. In retrieving section the primary secret image is disclosed by stacking the 2 shares, denoted by A XOR B, and therefore the second secret is discovered by initial rotating share A by angle ϴ anticlockwise.

B.For Color Images

- For Single Secret Sharing

From the 1997 visual cryptography schemes were applied to black and white pictures. Verheul and Van Tilborg developed colored visual cryptography scheme. The colored secret pictures are also shared using this method; the idea of arcs was accustomed construct a colored visual cryptography theme. In visual cryptography scheme one picture element is divided into m number of sub pixels, and every sub picture element is split into c color regions. In every sub picture element, there's precisely one color region colored, and every one the opposite color regions are black. The color of 1 picture element depends on the interrelations between the stacked sub pixels. For a colored visual cryptography theme with r colors, the picture element growth m is r× three. These schemes share generated were unimportant.

- Keyless Visual Cryptography

In this method the color image is take ,and the shares are generated using this method without any information of the first secret image and to retrieve the key image all the shares are required. The planned technique is enforced with the Seiving-Division-Shuffling rule planned in this paper and 3 steps. In the first step seiving the key image is split into primary colors. In step 2 Division these split pictures are haphazardly divided. In step 3 Shuffling these divided shares are then shuffled each inside itself to get final random share.

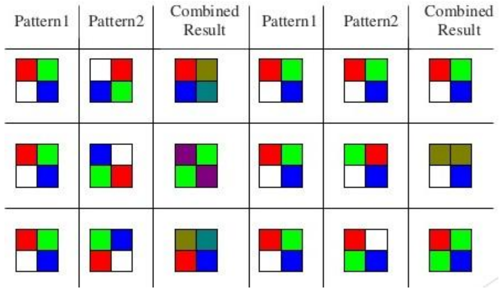


Figure.1 For color images

DOI 10.17148/IJARCCE.2019.8428

In above figure 1 each pixel is divided into 4 subpixel, such as color red,green,blue and white. After any order ,it gives the 24 different combination of color.We average the combination to present the color. For the encoding,it can choose the more closest combination, and select a random order from the first share.According to the combination,we can get the second share.

IV. PROPOSED SYSTEM

For phishing attack prevention, we are proposing a new methodology to prevent the website by phishing attack. The proposed methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It will allow only authenticated users to cast login. Also it will prevent phishing attacks in the internet websites. The proposed approach can be divided into two phases:

- **Registration Phase** :

During registration phase, end user has to provide user name, email ID for thesecure website. The user share is in form of images to provide more secure environment.Based on the information provided by the user, OTP and image captcha is randomlygenerated by server. The image captcha is divided into two shares, from that one share is kept with the user and the other share is kept in the server. The user'sshare and the original image along with OTP are sent to the user for later verificationduring login phase. The image and OTP is also stored in the actual database of any confidential website as confidential data. Because an image is used as the password for later. Registration process with sequence of encryption is depicted in below figure 2.

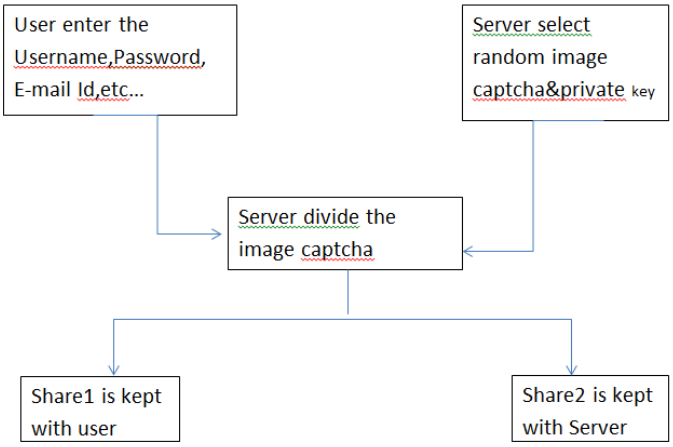

User enter the Username,Password, E-mail Id,etc...
Server select random image captcha&private key
Server divide the image captcha
Share1 is kept with user
Share2 is kept with Server

Figure 2.Registration phase

- Login Phase :

In the login phase, first user has to enter user name. Then user is asked to enter half share image which is kept with him/her. This share is sent to the server, after that the user's share and share which is stored in the database of the website, after that both the images is stacked together to generate the original image captcha. The generated image will be displayed to user and user can compare that generated image with the original image. At last the end user can check whether the displayed image captcha matches with the captcha which is created at the time of registration. If displayed images and captcha are same, user can complete the login process and user can generate the new OTP immediately when the login is successful otherwise user have to verify the website is genuine or fake.This phase is shown in below Figure 3.

DOI 10.17148/IJARCCE.2019.8428

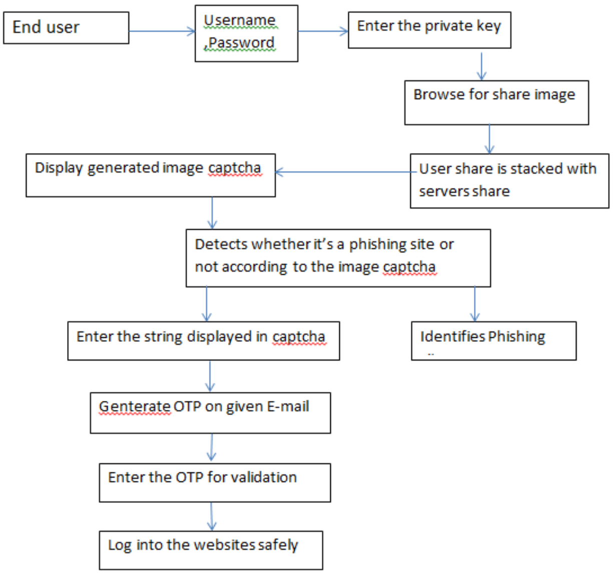

End user
Username ,Password
Enter the private key
Browse for share image
User share is stacked with servers share
Display generated image captcha
Detects whether it's a phishing site or not according to the image captcha
Enter the string displayed in captcha
Identifies Phishing
Genterate OTP on given E-mail
Enter the OTP for validation
Log into the websites safely

Figure 3.Login phase

A. Algorithm

1. Start
2. First input data as image and create an image graphics object by interpreting each element in a matrix.
3. Get the size of r as [c, p]
4. Get the plain Image
5. Get the mean of the plain Image
6. Compute the shared secret from the image
7. Iterate step 8 to 17 using secret key value
8. Extract the red component as r
9. Extract the green component as g
10. Extract the blue component as b
11. Let r =Transpose of r
12. Let g =Transpose of g
13. Let b =Transpose of b
14. Reshape r into (r, c, p)
15. Reshape g into (g, c, and p)
16. Reshape b into (b, c, and p)
17. Concatenate the arrays r, g, b into the same dimensionof r or g or b of the original image.
18. Finally the data will be converted into an image format to get the image

Where c, p are dimension of the image.[4]

B.Comparision between (2,2)VCS and (2,4)VCS

Table I.Comparision table

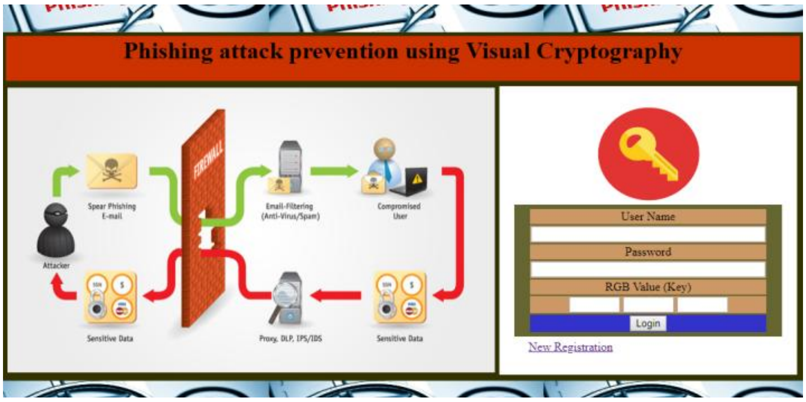
Comparative parameters	(2,2)VCS	(2,4)VCS
Image quality	Less	More
Number of share	2	4
Type of secrete	Random	Ramdom
Complexity	Less	More

DOI 10.17148/IJARCCE.2019.8428

In the above Table I it shows the comaprision between (2,2)VCS and (2,4)VCS of visual cryptography scheme.The creation and stacking of share is developed by using these scheme.

IV.RESULT

In the project , There are two phase one for registration of user and one for login of user,each have name and password. Below images shows the complete process.



Phishing attack prevention using Visual Cryptography

User Name

Password

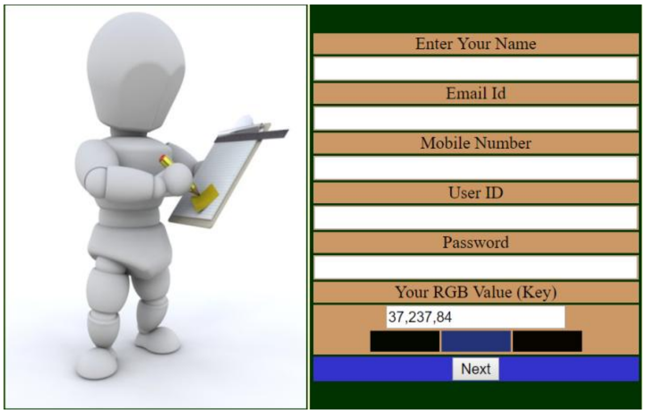
RGB Value (Key)

Login

New Registration

Figure 4.Home page

Figure 4 shows the home page in which it contain the registration link by clicking on that link the user can go for registration page.



Enter Your Name

Email Id

Mobile Number

User ID

Password

Your RGB Value (Key)

37,237,84

Next

Figure 5.Registration page

Figure 5.shows the registration page in which the user can do the registration

V.CONCLUSION

Phishing attack is more common in todays world because when it attacks it can capture and store user data information. Attackers use that data information wrongly. The proposed methodology can help to identify the phishing websites using visual cryptography, which preserves confidential information of user. Using visual cryptography two shares of the images are generated first share kept with the user and second share will be kept to server side along with that OTP will generate on user e-mail. The server has to request for user to enter image. Now server stacks its share two with user share one by visual cryptography. While checking if created picture is exact same as original one then only user can precede onwards otherwise if it is not match then phishing is captured and user session terminated. So it becomes strong security. As at the time of each login user is going to upload a image. To overcome such a problem it can provide alternating system to user by storing user share to server database only. And at the time of any login user will select one image given by the application server to user.

DOI 10.17148/IJARCCE.2019.8428

REFERENCES

[1]. Manasi Ashokrao Deshmukh, Prof. R. W. Deshpande, \Anti Phishing Website Using Visual Cryptography" in International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801 ISSN (Print): 2320-9798, Vol. 5,Issue 7, July 2017.

[2]. Sneha M. Shelke, Prachi A. Joshi, \Prevention of Phishing Threats using Visual Cryptography and One Time Password (OTP)" in International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Volume 5, Issue 2, February 2016.

[3]. Vikas Sahare, \Anti-Phishing System Using Visual Cryptography" in International Journal of Emerging Technologies in Engineering Research (IJETER), ISSN: 2454-6410, Volume 3, Issue 3, December (2015).

[4]. M. Hu and W. G. Tzeng , \Cheating Prevention in Visual Cryptography", IEEE Transaction on Image Processing, vol. 16, no. 1, pp. 36-45 (2007).

[5]. A. Eisen and D. R. Stinson , \Threshold Visual Cryptography with speci_ed Whiteness-Levels of Reconstructed Pixels, Designs, Codes, Cryptography", vol. 25, pp. 15-61 (2002).

[6]. Blundo and A. De Santis, \On the contrast in Visual Cryptography Schemes", Journal on Cryptography, vol. 12, pp. 261-289.

[7]. Anthony Y. Fu, Liu Wenyin, \Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Movers Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3, n 4, p301-311, October/December 2006

[8]. Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu, \An Antiphishing Strategy Based on Visual Similarity Assessment", IEEE Internet Computing, v 10, n 2,p 58-65, March/April 2006.

[9]. Haijun Zhang , Gang Liu, and Tommy W. S. Chow, \Textual and Visual Content-Based Anti-Phishing:A Bayesian Approach", IEEE Trans. Neural Netw., vol. 22, no. 10, pp.15321546, Oct. 2011.

DOI 10.17148/IJARCCE.2019.8428