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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

An Anti-phishing Framework using Visual Cryptography

Abhishek Thorat[1], Mahesh More[2], Ganesh Thombare[3], Vikram Takalkar[4], Manisha N.Galphade[5]

Student, Computer Department, Sinhgad Institute Of technology, Lonavala, India [1,2,3,4]

Associate Professor, Computer Department, Sinhgad Institute Of technology, Lonavala, India[5]

Abstract: In todays era, information security is an important aspect in which data is secure from unauthenticated user. Unsuspected victim attacks the information for economic gain, individual gain and for other illegal activities. Phishing is one of them in which unauthenticated person tries to thieve personal confidential information. To avoid these illegal activities we have projected a new paper "An Anti-Phishing Framework Using Visual Cryptography". In this, image is generated which after exploit, decomposed into two shares. One share is kept with user and other with server. And when it requires that is at the time of login at particular site two shares are combined together to form original image. The image form by combining two shares will state that current site is not a Phishing site and also identify that user is authenticated one. So data can be secured from unsuspected person.

Keywords: Visual Cryptography, Encryption, Phishing Attack, Shares, Security.

I. INTRODUCTION

Nowadays bank transaction e-commerce, online booking system, etc are very common. So various attacks can hazards the information used while performing above mentioned activities. Phishing is one of them in which illegal activities are performs using different social engineering techniques[1][3]. Attackers try to acquire important information such as password, credit card details and confidential data. Definition of phishing state that "Phishing is the fraud method in which sensitive information is acquired by masquerading as a trustworthy for his/her economic or individual gain". Communication channels such as websites, e-mails and instant messaging services are very popular so in these cases, phisher can easily thieve information of authorised users.So to avoid such scenario we need to overcome two problems. First one is to identify whether the site is phishing site or not and second problem is to identify whether the user is authorised or not.

So here introduce new technique which can be used as safety method against phishing which is named as" An Anti-Phishing Framework Using Visual Cryptography". In this method website verifies its own identity and prove that it is a genuine website and also checks the users identity to avoid phishing. The frame work supports complete web application security.The proposed system has three phases first phase deals with user registration[1][2]. While making registration one image is selected by user from application site then it is converted into two share images[2]. In second phase user get share one of image which is encrypted at the time of exploitation of original image. To secure the share one at user side, user assign a private key to that image which necessary at the time of transaction. In third phase if user want to do any transaction then user need to upload share one with private key set by user to share one , while at the other side application server automatically upload share two of original image[2][4]. Now application server have both shares, so applying Visual Cryptography Algorithm on both shares. By this we get the image as an output. Now server will check whether image formed is same as original image or not. If it is same then user is authorised. To check whether website is phishing site or not user cross check the formed image with the original one[2]. If formed image is not same as the original image then it states that the one of user or website is fake[4]. In this way both problems get overcome by using "An Anti-Phishing Framework Using Visual Cryptography" method.

II. PROJECT WORK

2.1 PROJECT OVERVIEW

To imitate web pages of actual website, fake web pages are created by unsuspected people. To overcome this difficulty two processing technique are used viz., image processing and EVCS (Extended Visual Cryptography Scheme)[2]. Image processing is a method in which processing of an input image and to get the output. Generated output either better form of original image or characteristics of input image. Proposed EVC scheme is expansion of one pixel in original image to four sub-pixelwhich can be selected to produce the required images for each share. It can be shown that the resulting scheme is perfectly secured so that no any share image leaks any information of the original secret image.

2.1.1 PROJECT SCOPE

- Main scope of our proposed system is to protect the online user from phishing attack using visual cryptography[1][2][4].
- Using Visual Cryptography, image based authentication is done.
- Visual Cryptography is used to decomposedan image into shares[2].
- Original image is formed by combining appropriate shares.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

- Finally it helps in preventing the confidential information and passwords from unsuspected victims.

2.2 EXISTING SYSTEM

Existing system include the techniques such as installation of key logger, screen capture, man in the middle attacks, tricking customers through e-mails and spam messages. To avoid this attacks existing technique like One Time Passwords, Personal Identification Number, text captcha can be used. But by using these existing techniques we are not able to analyse the phishing site and 100% accuracy is not reserved.

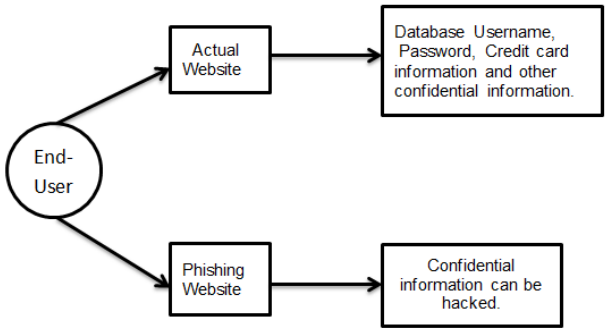

Figure 1-Current scenario

2.2.1 DISADVANTAGES

- To use OTP we always need sufficient mobile network to get OTP from server.
- Existing system does not give 100% accuracy.
- Exiting system is not able to detect whether the site is phishing site or not.

2.3 PROPOSED SYSTEM

As mentioned above the theory of image processing and enhance visual cryptography scheme is used. We divide our propose system into three phases which are mentioned below,

2.3.1 USER REGISTRATION PHASE

To do any online transaction one need to register to any bank which provide online banking.In this phase user registration is done with the help of Visual Cryptography Algorithm.While registration of user with visual cryptography user is provided by the random images that server have[4]. Among these images user select one image for visual cryptography. The selected image need to remember by the user which is needed in future. After the selection of image Visual Cryptography algorithm is applied on that image. Output of this phase will give two shares. Out of which first share goes under the process of phase two. And second share will recorded to server side with user id and original image.

2.3.2 APPLY THE ENCRYPTION ALGORITHM

Now user completed the phase one. We need to give share one to user with secure approach. For that we assign the private key to the encrypted image. And store the private key to server side. When user goes for any transaction need to upload the share one and to authenticate himself, he need to give that private key.By this phase server can be easily identified.

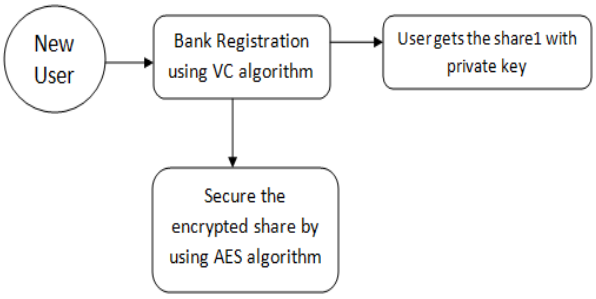

Figure 2-Login Phase

2.3.3DETECTION OF PHISHING SITE

When user goes for a transaction, user need to upload the share one[1][2][4]. After uploading, server will request for private key. User need to provide private key assigned during registration (in phase two). Now server is with share one and private key. Then server identify the user from that key. Now server stacks its share two with users share one by Visual Cryptography. A new image is formed from these two images. Server will check that image with the original one while user also checks formed image with original image selected in phase one[2].

If formed image is same as original image then proceed further transaction and if it is not phishing is detected and user can terminates the transaction without any loss of confidential data[1][4].

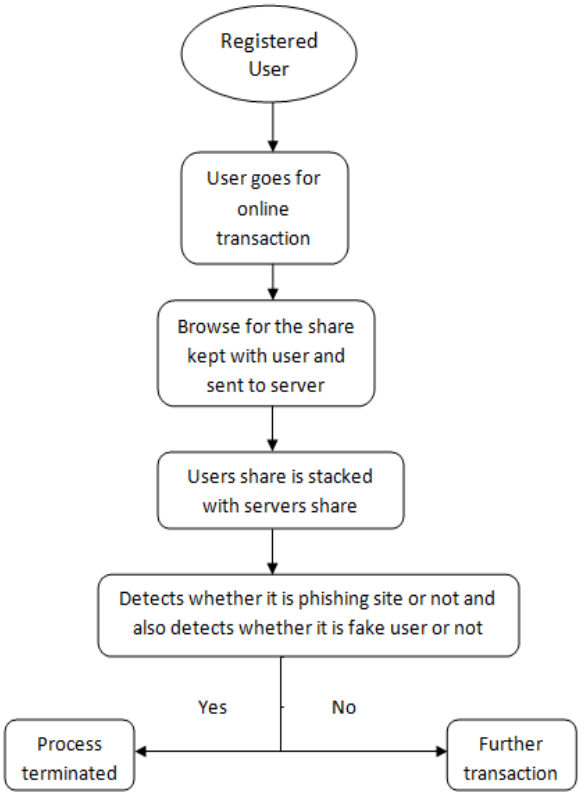

Figure 3-Detection Of Phishing Site

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

2.4 SYSTEM ARCHITECTURE

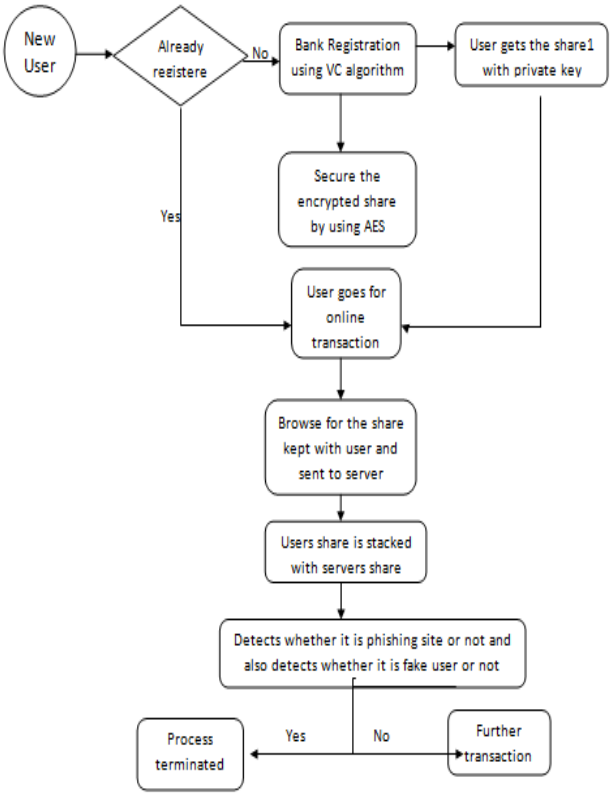

Figure 4-System Architecture

III. ALGORITHM AND TECHNIQUE USED

3.1 Balanced Block Replacement (BBR) –

1. Steps of grayscaleconversion [2]:
Step 1: Get dimension of the uploaded image
Step 2: Declare to variable X and Y representing x axis and y axis.
Step 3: Set initial position of X and Y to '0'
Step 4: increment the value of x and y by '1'
Step 5: get the pixel value of x and y
Step 6: check to which the pixel value is near-by to white or black
Step 7: change the value to black if it is near to black
Step 8: else change the value to the white if it is near to white
Step 9: repeat till all the pixels are converted.

2. Steps of encryption and decryption [2]:
Step 1: Get width and height of the image
Step 2: Horizontal block=image width/2
Step 3: Vertical block =image height/2
Step 4: Number of block = horizontal block X vertical block
Step 5: Encrypt all the pixels

3.2 ADVANCED ENCRYPTION STANDARDS (AES) -

- AES is a non-Feistel cipher that encrypts and decrypts a data block of 128-bits.
- The key size can be 128,192 or 256-bits.
- Private key is given to user when share1 is kept with user for secure sending of share1 from server to user.
- At the time of transactions, user need to enter the key for authentication process.
- After proper authentication, user is verified and goes for further process.

IV. DISCUSSION AND FUTURE WORK

Image formed and original image is related with the high degree of correlation. But by using Visual Cryptography Algorithm we get very low correlation coefficient. It is observed that by this method obtained correlation coefficient is -0.0073[1], which can be negligible. Hence this shows that there will be zero degree of correlational between original and output images for two different shares[1].

The proposed system is highly secured so it can be used in any online transaction like banking as mentioned in this paper[1][3][4][5]. Also this system can be implemented on online recharge system, online reservation system and so on.

In proposed system to complete the transaction user should have the encrypted part of image that is share one, means at the time of each transaction user is going to upload a image. To overcome such a problem we can provide alternating system to user by storing user share to server database only. And at the time of any transaction user will select one image given by the application server to user.

V. CONCLUSIONS

Phishing websites as well as human user can be easily identified using our proposed "An Anti-Phishing Framework Using Visual Cryptography" method. The proposed methodology preserved confidential information of user by using image share security. If the website is phishing web site then in that situation, the website can't generate original image for that specific user how wants to do transaction. The proposed methodology is also useful to prevent the attack on financial web portals, banking portal, e-commerce, online shopping, etc. Zero false positives and 100% true positives are generated by using our propose mechanism for detecting and preventing phishing attacks. The empiricalresults reveal that the proposed anti-phishing scheme is effective and can be used in real time applications.

ACKNOWLEDGEMENT

We are very grateful to all authors in reference section. Their methods, algorithms, conceptual techniques are very helpful for our research. All papers in the reference section are very useful for our proposed system.

REFERENCES

[1] Divyajames and Mintu Philip, A novel anti phishing framework based on Visual cryptography,978-1-4673-0449-8/12/$31.00©2012 IEEE.
[2] N.Askari, H.M. Heys and C.R.Moloney, An extended visual cryptography scheme for halftone images,2013 26thIEEE CCECE,978-1-4799-0033-6/13/$31.00©2013 IEEE
[3] Y.YesuJyothi,D.Srinivas,K.govindaraju, The secured anti phishing approach using image based validation,IJRCCT,Vol. 2,Issue 9,Sept 2013.
[4] K.A.Aravind,R.MuthuVenkataKrishnan, Anti-phishing framework for banking based on visual cryptography, IJCSMA , Vol. 2,Issue 1,Jan 2014, pg.121-126.
[5] MounikaReddy.M and MadhuraVani.B,, A novel anti phishing framework based on Visual cryptography, IJARCCE, Vol. 2,Issue 9, Sept 2013.