Anti-Phishing framework based on Extended Visual Cryptography and QR code

Shubhangi Khairnar
ME Scholar
Pimpri Chinchwad College of Engineering
Pune-44

ABSTRACT
Nowadays Online transactions are become very common and there are various attacks occur behind this. In these types of various attacks, phishing is very common attack. For detecting this attack various anti-phishing mechanisms are used. Propose a new authentication scheme for se-cure OTP distribution in phishing website detection through EVC and QR codes. The Website Detection using extended visual cryptography (EVC) technique and OTP to solve the problem of phishing. Here an image based authentication using extended visual cryptography is implemented with the combination of OTP (One Time Password). Image based QR codes authentication using EVC is used. The use of secret sharing technique is discovered to convert the QR code into two shares and both these shares can then be transmitted separately. One Time Passwords (OTP) is passwords which are valid only for a session to validate the user within a specified amount of time. The system provides high security requirements of the online users and protects them against various security attacks. Also the system is very user-friendly. It is reliable method for detecting phishing websites.

Keywords
OTP, Phishing, QR, Extended visual cryptography.

1. INTRODUCTION
Nowadays Online transactions become very common, various attacks present behind online transaction. Phishing is one type of attack, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so protective mechanism should also be so effective. Thus the security in these cases be very high and should not be easily controllable with implementation easiness.

Phishing was use to recognized the electronic Mail messages, designed to resemble messages from a reliable agent, such as a bank or online commerce site. These messages regularly request the user to take some form of action, such as validating their account information. These messages frequently use wisdom of urgency to motivate the user to take action. Now a days, there have been several new social engineering methods to cheat unsuspecting users while just a small portion of internet users have enough knowledge about different kinds of phishing.

Phishing has enormous bad impact on organizations' revenues, customer relationships, marketing efforts and overall corporate image [3]. Phishing attacks can cost companies tens to hundreds of thousands of dollars per attack in fraud-related losses and personnel time. Even worse, costs associated with the damage to brand image and consumer confidence can run into the millions of dollars [4].

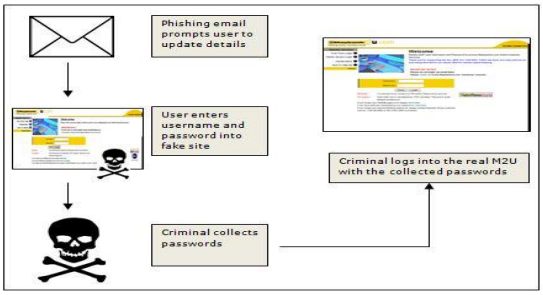

Fig.1 Phishing Process

Internet fraud has a multiplicity of forms, including Phishing attacks. Phishing is an attack that seeks to trick people into revealing sensitive information about themselves and their internet accounts [3]. Phishing aims to take advantage of the way humans interact with computers rather than taking advantage of technical system vulnerabilities [3]. Phishing is about other parties attempting to gain personal information such as bank details and passwords. As the Internet has become a vital medium of communication, Phishing can be performed in different ways. They are as follows:

1. email-to-email: this happens when someone receives an email asking for sensitive information to be replied to the sender email or sent to another email.
2. email-to-website: this happens when someone receives an email with embedded web address that leads to a Phishing website.
3. website-to-website: this happens when a Phishing website is reached by clicking on an online advert or through a search engine.
4. browser-to-website: this happens when someone misspelled a web address of a legitimate website on a browser and then goes to a Phishing website.

2. LITERATURE SURVEY
A. Novel Anti Phishing framework based on Visual Cryptography [2]:
This paper presents for phishing detection and prevention, this paper proposed a new methodology to identify the phishing website. This methodology was based on the Anti-Phishing Image Captcha Validation scheme using visual cryptography. This method prevents password and other important information from the phishing websites. This methodology was implemented image based authentication using Visual Cryptography. The use of visual cryptography is discovered to preserve the privacy of an image captcha by decomposing the original image Captcha into two shares that are stored in separate database servers such that the original image captcha can be discovered only when both shares are simultaneously

available; the individual shares images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Using this website cross verifies its identity and proves that it is a honest website before the end users.

B. An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection [7]:

This paper proposed a novel anti-Phishing approach that uses training intervention for Phishing websites detection. The proposed Methodology helps users to make correct decisions in distinguishing Phishing and genuine websites. It passes data to end-users and helps them instantly after they have made a mistake in order to recognize Phishing websites by themselves. This paper reports that there is a positive effect of using the new approach in judgment with an old approach of sending anti-Phishing advices by email. This approach is better in helping users correctly judge genuine and Phishing websites.

C. Online Payment System using Steganography and Visual Cryptography [5]:

This paper proposed a new approach for providing partial information only that is necessary for fund transfer during online shopping. The method uses the steganography and visual cryptography for prevent the user confidential information. In the proposed method, used the text based steganography for hiding the customer unique authentication password in connection to the bank. This system use to protect customer data and increasing customer assurance and preventing identity theft. Customer authentication information in connection with merchant is placed above the cover text in its original form. Now give the snapshot of two texts. From the snapshot image, using visual cryptography two shares are generated. This method use to preserved customer data privacy and prevents misuse of data at merchant's side. The method is concerned only with prevention of detect theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography, are mainly applied for physical banking, the proposed method can be applied for online shopping as well as physical banking.

D. an Efficient Approach for Phishing Website Detection using Visual Cryptography (VC) and Quick Response Code (QR Code) [14]:

In this paper proposed image based authentication using Visual Cryptography is used. Visual cryptography is use to transform the QR code into two shares and both these shares can then be transmitted separately. In this paper doing comparison of this paper with the existing system and show how this method is more efficient and also show the results. The comparison between existing and proposed system we prove that this method is more efficient and secured. In recent years increase the number of online users. Hence the proposed system fulfills the high security requirements of the online users and protects them against various security attacks. Also the system is very user-friendly. Hence QR code proves to be versatile at the same time helpful for both the customers in terms of security and vendors in terms of increasing their efficiency.

E. Malicious Website Detection using Visual Cryptography and OTP [11]:

This paper proposed a new method "Malicious Website Detection using Visual Cryptography and OTP" use to solve the problem of phishing. In this approach image based authentication using Visual Cryptography is implemented with the combination of OTP. The use of visual cryptography is discovered to preserve the secrecy of an image captcha by dividing the original image captcha into two shares. The original image is gained at the user end only when both the user and the server are registered with the trusted server. Using this, website cross verifies its identity and proves that it is a honest website before the end users. This paper can easily identify the phishing websites. This proposed technique provides more security as a random OTP is chosen for a particular session and the visual cryptography is done on the genuine server side. Since the generated shares are valid for a particular session and are not stored on server or user, there is no chance of the share getting taken by any other user. Hence it provides much better security.

F. An Enhanced Anti-Phishing Framework Based on Visual Cryptography [15]:

In this paper proposed a new technique "An Enhanced Anti-Phishing Framework Based on Visual Cryptography". In this paper an image based authentication using Visual Cryptography is implemented. This proposed technique uses visual cryptography to preserve the privacy of the randomly chosen image by dividing the image into two shares. These two shares are for that particular session. Using this method the user can determine whether the site is safe or unsafe to carry out his transaction.in this methodology first of all the user gets registered with the trusted server. The trusted server stores unique keys for the users required for decryption of the share. The original image is obtained at the user end only when both the user and the server under test are registered with the trusted server. If original image is obtained then the server under test is a genuine server otherwise close the session. Original image is obtained if and only if both user and the server under test are registered with the trusted server. If either of the user or server under test is not registered with the trusted server then an improper image is obtained.

3. PROPOSED WORK

In some applications like defense, important information, banking transaction needs to be transmitted in the form of secret. This information may be lost during the transmission. To get the security and reliability secret sharing can be applied in such applications. Sometimes the shares may be lost in transmission or dishonest participants can modify their shares. In such scenarios verifiability is required for the reconstructed secret which will assure the participants about the accuracy of retrieved secret. Proposed system is shown in fig.2

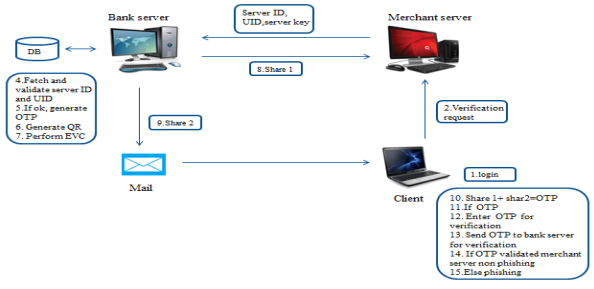

Fig 2. Architecture of Proposed Work

In proposed system user does registration process first. Send request to merchant server and merchant server send ID and password to bank server for verification. If it is valid then generate OTP and apply EVC for shares generation. Send one share to client and one share to server. Then merchant server sends this share to client. At the time of reconstruction

combine this two shares revel the original OTP.Then send this OTP to bank server for verification.

A. Grayscale Algorithm
Steps:

- Read Image
- Get height and width of image
- for (x to h)

  for (y to w)
- Read RGB pixels of locations x and y
- Separate R , G , B
- gs= r+g+b/3
- Set gs value to all RGB values.
- Apply thresholding

```
if (gs < 128)
{
  R=G=B= 0;
}
else
{
   R=G=B= 1;
}
```

B. Share Generation Algorithm

Steps:

- Read Image (QR image)
- Get height and width of that image.
- Apply cryptography :

  1] Create share 1 by generating random (2*2) matrix

  2] Fill this matrix (0, 1) using random value.
- Share 1 XOR with pixel of original image.
- Share 2 is created.

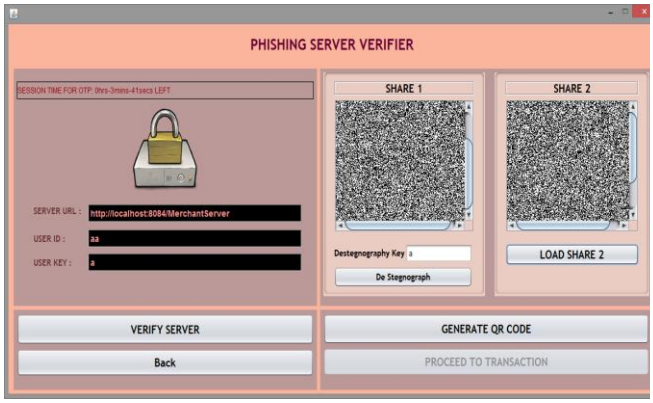

Fig 5. Snapshot for share generation after adding cover image

Fig 6. Snapshot for QR code generation

4. CONCLUSION

In this paper different Online Fraud Transaction prevention system is studied based visual cryptography. From study we proposed a method for Online Fraud Transaction prevention using EVC and QR code techniques. In previous system cannot verify the shares are genuine or not but by using EVC we can verify the shares and provide better security than previous system. The system provides high security requirements of the online users and protects them against various security attacks. Also the system is very user-friendly. It is reliable method for detecting phishing websites.

5. REFERENCES

[1] M. Noar, A. Shamir, “Visual cryptography,” in: A. De Santis (Ed.),Advance in Cryptography: Eurpocrypt’94, Lecture Notes in Computer Science, Volume. 950, pp. 1-12, 1955.

[2] Divya James, Mintu Philip, “A Novel Anti Phishing framework based on Visual Cryptography’ 978-1-4673-0449-8/12/$31.00 ©2012 IEEE.

[3] J.W. Ragucci and S. A. Robila, “Societal Aspects of Phishing, in technology and Society, 2006. ISTAS 2006. IEEE International Symposium on, 2006, pp. 1 –5.

[4] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, “Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies,” Cognitive Computation, vol. 2, no. 3, pp. 242–253, Apr. 2010.

[5] Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," 2014 IEEE Students’ Conference on Electrical, Electronics and Computer Science

[6] Giuseppe Ateniese, Carlo Blundo,” Extended Capabilities for Visual Cryptography”, Department of combinatorics and Optimization University of waterloo, N2L, 3G1, Canada.

[7] A. Alnajim and M. Munro, “An anti-phishing approach that uses training intervention for Phishing websites detection,” in Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations. Washington, DC, USA: IEEE Computer Society, 2009, pp. 405–410.

[8] J.S. Downs, M. B. Holbrook and L. F. Cranor, “Decision strategies and susceptibility to phishing”. Proc. the 2nd

symposium on usable privacy and security. New York, USA: ACM Press, 2006, pp. 79 – 90.

[9] M. Chandrasekaran, R. Chinchani and S. Upadhyaya,"PHONEY: Mimicking User Response to Detect Phishing Attacks". Proc. International Symposium on a World of Wireless, Mobile and Multimedia Networks. Washington DC: IEEE Computer Society, 2006, pp. 668-672.

[10] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[11] Kajal NanawareÀ, Kirti KanadeÀ, "Malicious Website Detection using Visual Cryptography and OTP", International Journal of Current Engineering and Technology, Vol.4, No.5 (Oct 2014)

[12] 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.

[13] D. R. Anekar, Binay Rana, Vishal Jhangiani," Online Banking Security System Using OTP Encoded in QR-Code ", 2015, IJARCSSE

[14] Dhanashree Moholkar ,"An Efficient Approach for Phishing Website Detection using Visual Cryptography (VC) and Quick Response Code (QR Code)", International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 12, April 2015

[15] Gaurav Palande, Shekhar Jadhav," An Enhanced Anti-Phishing Framework Based on Visual Cryptography", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-3)