PROBABILISTIC MODEL OF VISUAL CRYPTOGRAPHY AND IMAGE ENCRYPTION SCHEME

$M.Kaliraj$[1] , P.Manimannan[2],$V.Gopinath$[3]
[1]BE 4th year Computer Science and Engg, [2]BE 4th year Computer Science and Engg
, [3] Assistant Prof. Dept.of Computer Science and Engg
Arjun College of Technology, Coimbatore, Tamilnadu, India.

ABSTRACT

Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities. The first defense should be strengthening the authentication mechanism in a web application. A simple username and password based authentication is not sufficient for web sites providing critical financial transactions. In this paper we have proposed a new approach for phishing websites classification to solve the problem of phishing. Phishing websites comprise a variety of cues within its content-parts as well as the browser-based security indicators provided along with the website. It is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha.It can be revealed only when both are simultaneously available. The individual sheet 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. Several solutions have been proposed to tackle phishing. “Anti-phishing using visual cryptography". As the name describes, in this approach website cross verifies its own identity and proves that it is a genuine website to use bank transaction, E-commerce and online booking system etc. before the end users and make the both the sides of the system secure as well as an authenticated one.

I. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective. Thus the security in these cases be very high and should not be easily tractable with implementation easiness. Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security.

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. One definition of phishing is given as “it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication”. The conduct of identity theft with this acquired sensitive information has also become easier with the use of technology and identity theft can be described as "a crime in which the impostor obtains key pieces of information such as Social Security and driver's license numbers and uses them for his or her own gain". Phishing attacks rely upon a mix of technical deceit and social engineering practices. In the majority of cases the phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information.

II. RELATED WORK

Phishing web pages are forged web pages that are created by malicious people to mimic Web pages of real web sites. Most of these kinds of web pages have high visual similarities to scam their victims. Some of these kinds of web pages look exactly like the real ones. Victims of phishing web pages may expose their bank account, password, credit card number, or other important information to the phishing web page owners. It includes techniques such as tricking customers through email and spam messages, man in the middle attacks, installation of key loggers and screen captures.

III. PROPOSED SYSTEM

The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. In Visual Cryptography (VC) an image is decomposed into shares and in order to reveal the original image appropriate number of shares should be combined.VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

The modules are as follows:

- Registration With Secrete Code
- Image captcha Generation
- Shares Creation(VCS)
- Login Phase

MODULE DESCRIPTION

A. REGISTRATION WITH SECRETE CODE

In the registration phase, the user details user name, password, Email-id, address and a key string (password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server. The key string can be a combination of alphabets and numbers to provide more secure environment.

B. IMAGE CAPTCHA GENERATION

A key string is converted into image using java classes Buffered Image and Graphics2D. The image dimension is 260*60.Text color is red and the background color is white. Text font is set by Font class in java. After image generation it will be write into the user key folder in the server using Image class. A key string is converted into image using java classes Buffered Image and Graphics2D. The image dimension is 260*60.Text color is red and the background color is white. Text font is set by Font class in java. After image generation it will be write into the user key folder in the server using Image class.

C. SHARES CREATION (VCS)

The image captcha is divided into two shares such that one of the shares is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data.

D. LOGIN PHASE

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website.

SYSTEM ARCHITECTURE

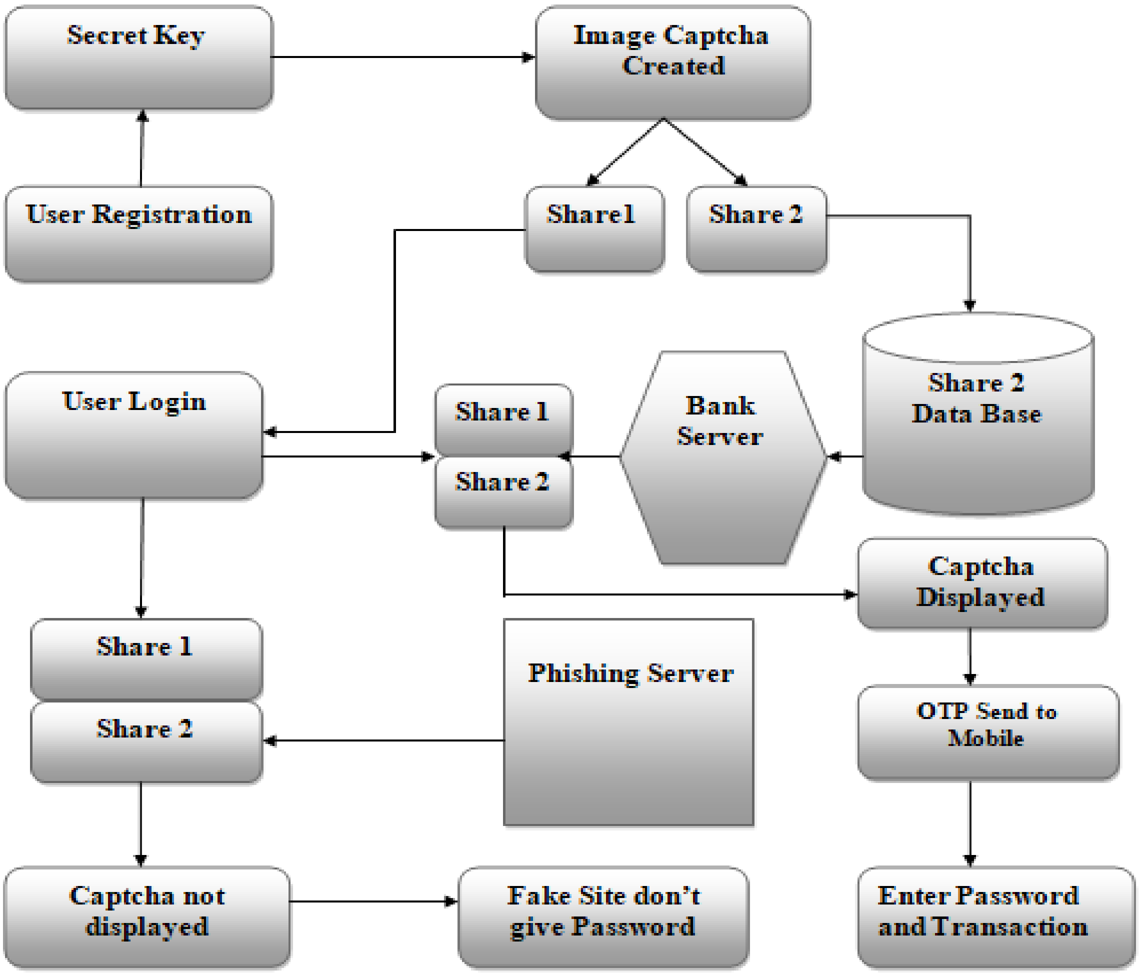

Figure System Architecture

IV. CONCLUSION AND FUTURE WORK

The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market. Currently phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using our proposed "Anti-phishing framework based on Visual Cryptography". The methodology preserves confidential information of users. Verifies whether the website is a genuine/secure website or a phishing website. If the website is a phishing website (website that is a fake one just similar to secure website but not the secure website), then in that situation, the phishing website can't display the image captcha for that specific user due to the fact that the image captcha is generated by the stacking of two shares, one with the user and the other with the actual database of the website.

In future we can increase the security by adding many algorithms to encrypt the image. Encryption Phase contains many algorithms like Blowfish, Splitting and Rotating algorithm and Visual Cryptography Scheme. First the "Blowfish Algorithm" is applied to the original image captcha then the image captcha is divided into many blocks and rearranged. After the image captcha blocks are rearranged, the "Splitting and Rotating Algorithm" is applied to the image captcha, and then the rearranged blocks are rotated.

REFERENCES

[1] A S. Agaian, C. L. P. Chen K. Panetta and Y.Zhou, "(n, k, p)-gray code for image systems," IEEE Trans. Cybern., vol. 43, no. 2, pp. 515–529, Apr. 2013.

[2] H. Chen, X. Du, Z. Liu, and C. Yang, "Color image encryption based on the affine transform and gyrator transform," Opt. Lasers Eng., vol. 51, no. 6, pp. 768–775, 2013.

[3] C. L. P. Chen, Z. Hua, C.-M. Pun and Y. Zhou "Cascade chaotic system with applications," IEEE Trans. Cybern., vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[4] A. Jolfaei, V. Muthukumarasamy and X.-W. Wu "On the security of permutation-only image encryption schemes," IEEE Trans. Inf. Forensics Security, vol. 11, no. 2, pp. 235–246, Feb. *2016*.

[5] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," Opt. Commun., vol. 284, nos. 16–17, pp. 3895–3903, 2011.

[6] Y. Liu, J. Wang, K.-W. Wong, and L. Y. Zhang and "Chosen plaintext attack of an image encryption scheme based on modified permutation–diffusion structure," Nonlin. Dyn. vol. 84, no. 4, pp. 2241–2250, 2016

[7] W. Li, Y. Yan, and N. Yu, "Breaking row-column shuffle based image cipher," in Proc. 20th ACM Int. Conf. Multimedia, Nara, Japan, 2012, pp. 1097–1100.

[8] Q.X. Pan, S.-J. Sun, and P. Xu and Y.-G. Yang "Novel image encryption based on quantum walks," Sci. Rep., vol. 5, no. 7, 2015, Art. No. 7784.

[9] L. Yang, C. Zhao, X. Zhang, and H. Zhu, "An image encryption scheme using generalized Arnold map and affine cipher," Optik Int. J. Light Electron Opt., vol. 125, no. 22, pp. 6672–6677, 2014.

[10] C. Zhu and C. Zhao, "A novel image encryption scheme based on improved hyperchaotic sequences," Op