Research Paper Engineering

Anti-Phishing Framework Using Image Captcha Authentication Based on Visual Cryptography

* Latha Yadav T.R. ** Manjula B.K.

* PG Student, Department of ECE, GM Institute of Technology

** Assistant professor, Department of ECE, G M Institute of technology

ABSTRACT

The growth of internet has resulted in global sharing of information. In this age of internet how to keep the information secret is always an important issue. There are many threats that computer systems and users face on the internet. Among the various threats phishing is identified as a major one. Phishing is the act of attempting to acquire the confidential informations such as username, password, credit card details and so on by masquerading as a trustworthy entity in an electronic communication. In this paper we have proposed a new approach named as "Image Captcha Authentication Based on Visual cryptography". So by using the visual cryptography scheme the original image captcha is decomposed into two shares that are stored in separate database server such that one with the server and other with the user. The individual share do not reveal the image captcha.

Keywords : Phishing, image captcha , shares

I. Introduction

Online services simplify our lives. They allow us to access information ubiquitously and are also useful for services providers because they reduce the operational costs involved in offering a service. For example, online banking over web has become indispensable for customers as well as banks. Unfortunately, interacting with an online service such as banking web application often requires a certain degree of technical sophistication that not all Internet users possess. For the last couple of years, such naive users have been increasingly targeted by phishing attacks that are launched by miscreants who are aiming to make an easy profit by means of illegal financial transactions.

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. So a better system is required to counter phishing attacks effectively and efficiently.

Later, 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

This paper is organized as follows: Section II and section III presents the current and proposed methodologies. Section IV presents the implementation and Section V contains the conclusion.

II. Current Methodology

In the current scenario as shown in the Fig. 1, when the end user wants to access his confidential information online by logging into his bank account or secure mail account, the person enters information like username, password, credit card no. etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques. There is no such information that cannot be directly obtained from the user at the time of his login input.

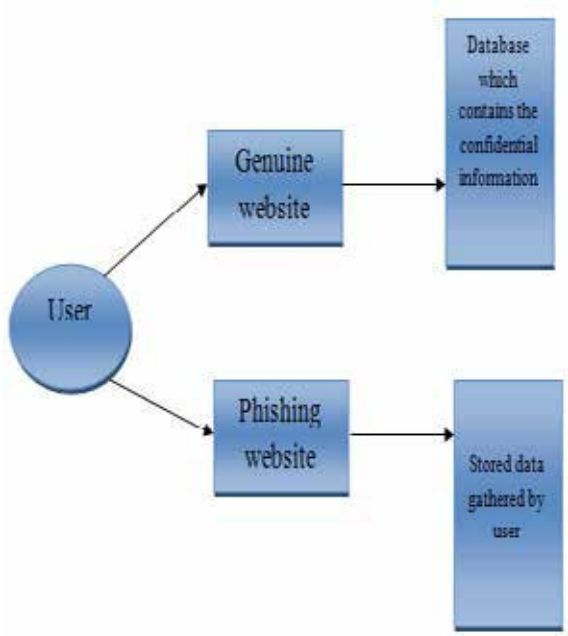

Figure1: Current scenario

III. Proposed Methodology

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on Image Captcha Authentication Based on

Visual cryptography scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.

The proposed approach can be divided into two phases:
- Registration Phase
- Login Phase

- **Registration Phase**

In the registration phase, 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 and an image captcha is generated.

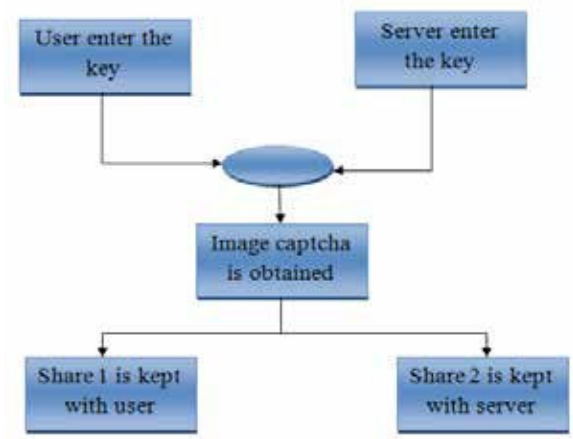

Fig.2: When user performs registration process for the website

The image captcha is divided into two shares such that one of the share 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. After the registration, the user can change the key string when it is needed. Registration process is depicted in Fig.2 and Fig.3 shows the resulting page of the registration phase where the user is going to enter his details when he is going to register.

Fig.3: Resulting page of the registration phase

- **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. The image captcha is displayed to the user. Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. 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 and can also verify whether the user is a human user or not. This phase is depicted in Fig.4 shows the overview of the login page and Fig.5 shows the resulting page of login page.

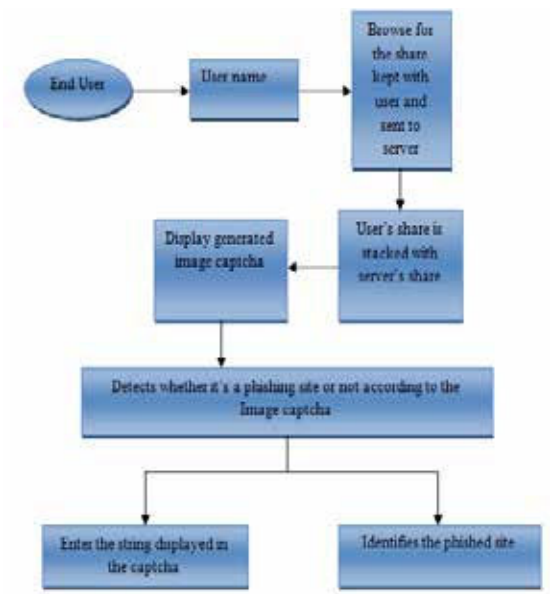

Fig.4: When user attempts to log in into site

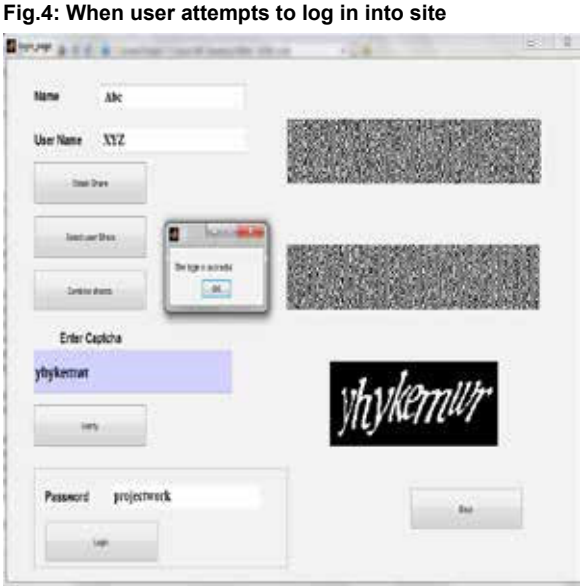

Fig.5 Resulting page of the Login phase

IV. Implementation and Analysis

The proposed methodology is implemented using Matlab. Fig 6, shows the result of creation and stacking of shares.

In the registration phase the most important part is the creation of shares from the image captcha where one share is kept with the user and other share can be kept with the server.

In the login phase, the user needs to enter a valid username in the given field. Then he has to browse his share and process. At the server side the user's share is combined with the share in the server and an image captcha is generated. The user has to enter the text from the image captcha in the required field in order to log in into the website.

The entire process is depicted in Fig.4 as differentcases. Case1 and Case 2 illustrates the creation and stacking of shares of two image captcha's resulting in original captcha. In Case3 share1 of first image captcha (Case.1) is combined with share2 of second captcha (Case.2) resulting in an unrecognizable form of captcha.

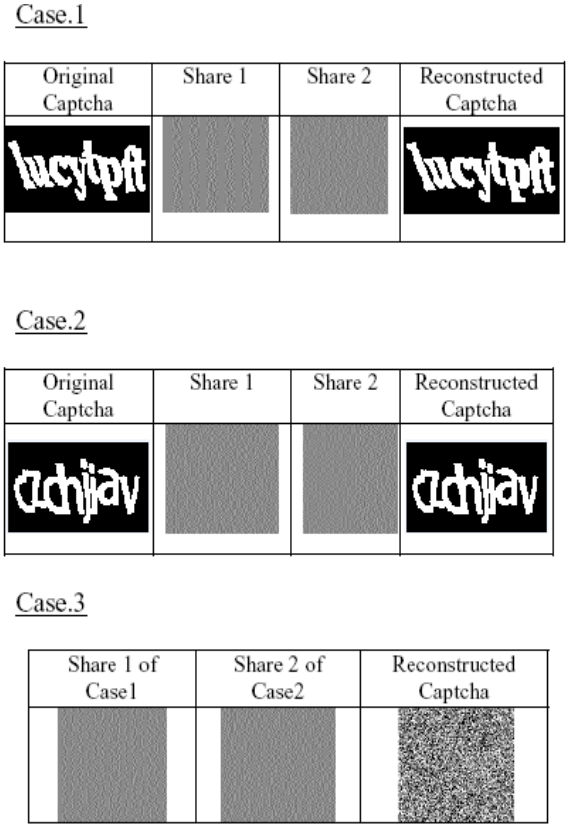

Fig. 6: Creation and stacking of shares

V. Conclusion

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 "Image Captcha Authentication Based on Visual cryptography". The proposed methodology preserves confidential information of users using 3 layers of security. 1st layer 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 (who wants to log in into the website) 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. Second layer cross validates image Captcha corresponding to the user. The image Captcha is readable by human users alone and not by machine users. Only human users accessing the website can read the image Captcha and ensure that the site as well as the user is permitted one or not. So, using image Captcha technique, no machine based user can crack the password or other confidential information of the users. And as a third layer of security it prevents intruders' attacks on the user's account. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

REFERENCES

[1]A Novel Anti Phishing Framework Based on Visual Cryptography, 2012, Divya James, Mintu Philip.
[2] Anti-Phishing Group of the City University of Hong Kong, [Obnline] Available: http://www.antiphishing.cs.cityu.edu.hk,2005
[3]Ollmann G., The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.
[4] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT,1994, pp. 1–12.
[5] A. Shamir, .How to Share a Secret,. Communication ACM, vol. 22, 1979, pp. 612-613.
[6] CAPTCHA: Using Hard AI Problems For Security Luis von Ahn1, Manuel Blum1, Nicholas J. Hopper1, and John Langford.