A Review of a Novel Anti-phishing Framework Based on Visual Cryptography

Vaishnavi Bahuriya, Upendra Malekar, Snehal Pidurkar

Student, Dept. of CSE, Ballarpur Institute of Technology, Gondwana University, MS, India

Assistant Professor, Dept. of CSE, Ballarpur Institute of Technology, Gondwana University, MS, India

Student, Dept. of CSE, Ballarpur Institute of Technology, Gondwana University, MS, India

ABSTRACT: Due to the overwhelming use of internet today in the field of online trades, internet attack has increased drastically. Among which the phishing is the most popular attack. Phishing is methods in which someone's sensitive information can be rob such as password, account details or credit card information. Fake website is the basic source of phishing attack. To overcome from this type of attack a new approach is proposed. By the use of visual cryptography technique the privacy of image captcha is been preserved by breaking down the original image captcha into two shares knows as sheets that are stored in separate database servers such that the original image can be disclosed only when both are simultaneously available. When the original image captcha is revealed to the user it can be used as the password, using this website can be verified whether it is phishing site or not.

KEYWORDS: Phishing, visual cryptography, security, image captcha, shares.

I. INTRODUCTION

In day to day world, online trades and commercial transaction are becoming very common and there is various security threats present behind this. Among the various threats, phishing is the most serious threats which is been used by the hackers. In each second various new innovative ideas of hacking are arising so the preventive mechanism must also be effective. Thus the security must be very strong so that hacker could not able to hack it.

A most of the application are secure as their respective system but the technology has been increased so far that their detection is a difficult problem. Due to this it's becoming impossible to trust any of the website. Now, here the question arises how to handle such application which need high security.

Basically, phishing is a type of theft that takes the user's confidential and private information which can be either password or account details. One can interpret phishing as criminal activities using social engineering methods. Phishing is done by the fraud people to steal the sensitive information such as password, OTP etc by sending an email which appear to be original site of any trusted source for the purpose of hacking.

For the purpose of the user safety, here we introduce a method against phishing which is been carried out by unique approach by using visual cryptography technique. As a name says, it is an approach which checks the particular site is safe or fraud site before the end user add all its sensitive information and make the site secure for the user which is to be used.

In this technique image processing concept is used. The input image is been processed in image processing and the output is the improved or same characteristic of the original image. In visual cryptography technique an image is split up into shares and in order to get the original image the particular number of shares should be combined. So there are various methods and we have discussed them in this paper along with their pros and cons.

II. RELATED WORK

In the year 2000, Ren-junn Hwang has given a technique which uses watermark method [1] to save the digital image copyright ownership. This method uses visual cryptography. In this method watermark pattern can be identified

without any information of the original message. But in this method there is the difficulty of detecting the pixels concentrating the watermark pattern without the secret key.

In the year 2012, DivyaJames [2] and MintuPhilip [2] has used visual cryptography technique [3] for their Anti phishing framework. They have given Anti phishing image captcha validation scheme which make use of visual cryptography. However this method is partitioned into two phases. One is the registration phase while other is the login phase. In first phase key string is used as password registration and this key string can be alphabets or numbers or concatenation of both with random strings generated in the server. The image captcha is formed using this key string. Further in Second phase user enters username and their login share and server generates a new image captcha which is to be same as the one generated during registration phase. The most important part is the creation of shares in the registration phase and the generation of the text in the image captcha in the login phase. Thus this technique verifies authenticity of websites cross verifies the image captcha and prevents attacks on user account.
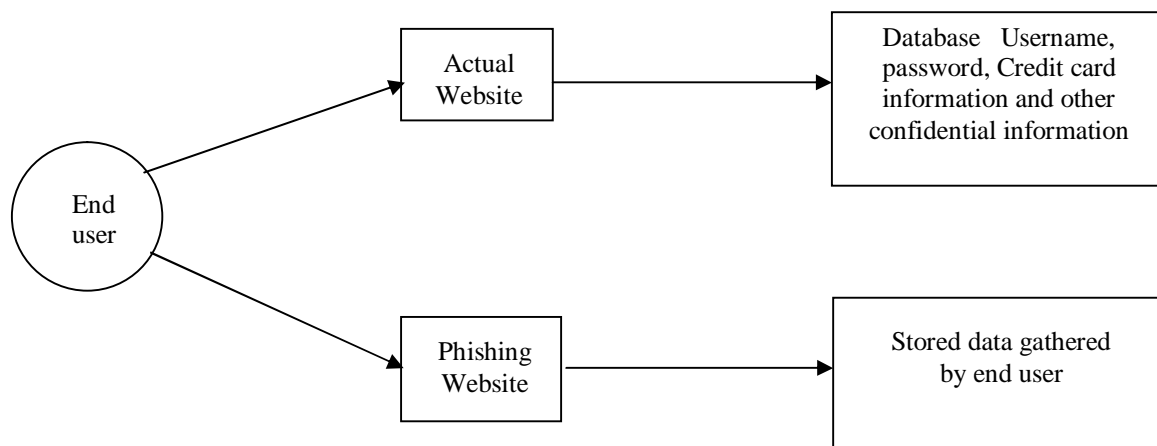
III. EXISTING METHODOLOGY

Fig1: Existing Scenario

In the existing scenario as depicted in the diagram whenever the end user performs an activity to access his confidential information online such as by login into his bank account or mail account ,the user enters details like username, password etc on the login phase. In some situation this information can be captured by hackers using phishing techniques.

IV. PROPOSED METHODOLOGY

For detecting phishing websites and prevention, we are giving a new methodology to detect phishing website. Our technique is based on the Anti -phishing image captcha validation scheme using visual cryptography. It preserves password and other confidential information from phishing websites.

We proposed the concept of image processing and visual cryptography. Image processing is the technique where the quality of output image is improved and in visual cryptography, the original image decomposed into two shares and to obtain the original image sufficient number of shares should combined.

V. MODULES

There are two modules included:
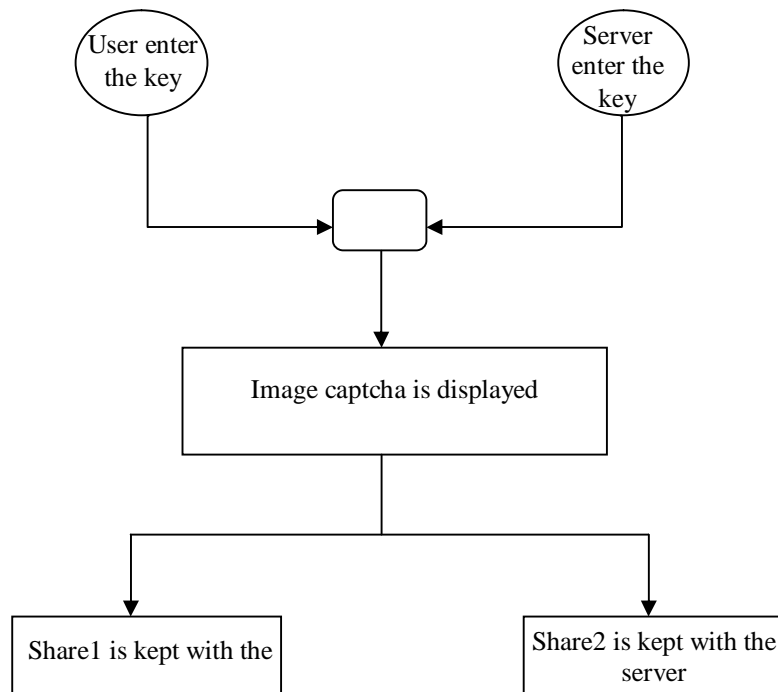1) Registration module
2) Login module

1. Registration phase

Fig 2: User registration on website

In the registration module, a key string i.e. password is asked to the user at the time of registration for the secure website. The given password can be a union of alphabets and numbers so as to provide secure environment. The given string is further concatenated with the randomly generated string by the server and by this image captcha is formed. This image captcha is now split-up into two shares such that one share is kept with user and another one with server. 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 (password) when it is required.

2. Login phase

In the Login phase first the user is asked for the username or user id. After this user is asked to enter his share which is kept with him. This share is then sent to the server where the user's share and the share which is stored in the database of the confidential website, for each user, is the stacked together to produce the image captcha. Now the image captcha is displayed to the user and here the end user check whether the given or the displayed image captcha matches with the captcha created at the time of registration. The end user is now required to enter the text displayed in the image captcha and this will be considered as a password and using this the user can log in into the secured website. Using the username and image captcha generated by stacking two shares one can verify whether the website is secured website or not and can also verify whether the user is a human user or not.
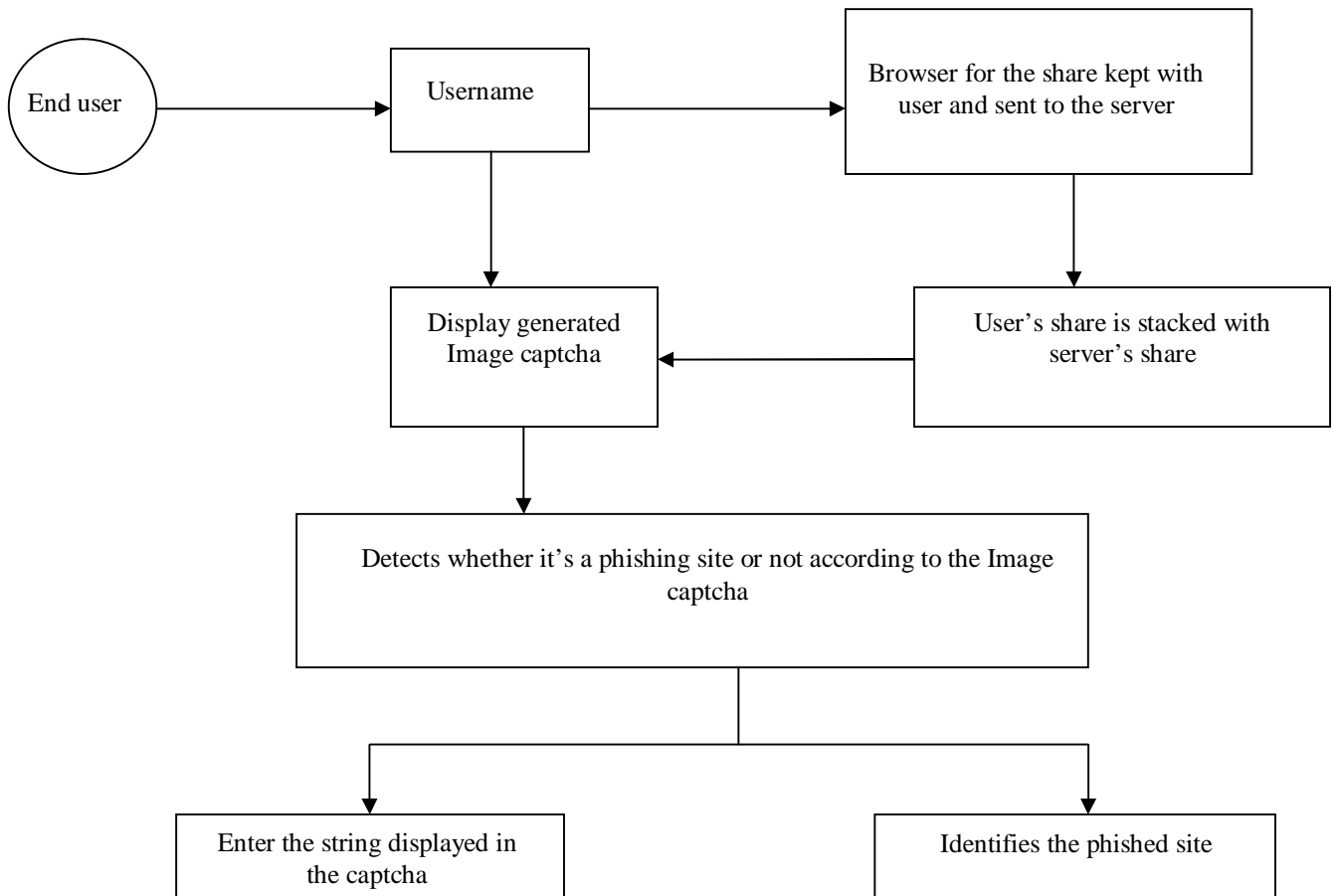
Fig 3: When user attempts to log in into site

VI. CONCLUSION

The cyber-crime is rapidly increasing day today. The intelligent hackers are making bogus or fake websites equal to the real websites and capture and store the user's personal or important information. By using our system we can overcome the drawbacks of above situation. This System helps to identify that the system is real or fake and if it is fake then the user's important information will not be shown to the phishing sites. The use of shares as a security key increases a high security level in our system. This system can be used in the different sectors such as banks,online shopping,marketing etc.

REFERENCES

1. Ren-JunnHwang,"A digital image copyright protection scheme based on visual cryptography", Tamkang Journal of science and engineering, Vol.3, No. 2, pp. 97-106(2000).
2. Divya James, MintuPhilip,"A novel Anti-phishing framework based on visual cryptography", IEEE 2012.
3. M.Naor and A.Shamir,"Visual cryptography", in Proc. EUROCRYPT, 1994, pp.1-12. IJDPS Vol.3, No.1, 2012.

BIOGRAPHY

Vaishnavi Bahuriya is a UG student of Computer Science and Engineering Department, Ballarpur Institute of Technology, Gondwana University. Her research interests are Computer Networks.

Upendra Malekar is an Assistant Professor in the Computer Science and Engineering Department, Ballarpur Institute of Technology, Gondwana University. He received Master of Engineering (ME) degree in 2015 from MIT Pune, University of Pune, MS, India. His research interests are Computer Networks (wireless Networks), Delay Tolerant Networks and Cloud Computing.

Snehal Pidurkar is a UG student of Computer Science and Engineering Department, Ballarpur Institute of Technology, Gondwana University. Her research interest are Computer Networks.