IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Security System for Online Transaction

Amol More[1], Archana Karbhari[2], Prem Gorivale[3], Sridhar Iyer[4]

UG Student, Computer science, Universal College of Engineering, Mumbai, India[1,2,3]

Assistant Professor, Computer science, Universal College of Engineering, Mumbai, India[4]

Abstract: Phishing is one of the assaults that have become famous these days. It's a type of robbery tried with an intention to obtain exclusive and private data of people or companies for monetary or other profits. Inside the latest component there had been many reports on phishing assault in lots of financial domains; such as banking. It has emerged as a severe threat to establishments that deal with monetary transactions. If those threats aren't addressed thoroughly, people can't trust on-line transactions that contain due authentication through credentials. Many solutions came to resolve this kind of identity robbery. We aim to develop a new approach based on visual cryptography to cope with this issue of phishing. This can automatically preserve the privacy of captcha. It achieves this through dividing the original photograph into two shares which might to be saved in one of a kind database. The decryption is possible best when adversaries can provide both shares at a time. The character shares can't display the authentic captcha. The planned frame work has two phases. Within the first phase, a brand new user registers himself. When the new user is processing for the registration, the net application chooses a picture; then the picture is split into two share pictures. Where as in authentication phase, the same user is asked for the share allotted him during registration phase. Solely the shares are accessible only with the original user. Therefore this phishing attacks can be effectively prevented.

Keywords: Visual cryptography, captcha, phishing, security, online transaction.

I. INTRODUCTION

Due to the invention of latest technologies over web online transactions has become a common feature in several web applications as well as e-commerce applications. As the transaction over web grows, the likelihood of security threats conjointly grows. One such threat is phishing attack that can perform fraud [1].Phishing may be a method of deceiving a party so as to get credentials and gain financial and other gains. Thus it is essential to create methodology needed to forestall such attacks. Phishing attacks are recorded within the history in banking and e-commerce domains. By stealing identity details of on-line users one will gain access to original internet application and perform activities that there were not approved. Phishing is one amongst the fraud attacks that square measure to be handled with efficiency. There have been several solutions. This framework supports complete internet application security with the reference to the phishing attacks involved. The planned framework has 2 phases. Within the 1st phase, a replacement user registers himself. Whereas he is creating registration the online application chooses a picture then it's converted into 2 share pictures. Whereas in authentication phase, the user is asked for the2 shares. Solely the shares are obtainable with original user solely. So the phishing attacks square measure effectively prevented. The popular technologies that deal with phishing problem have several drawbacks: Blacklist-based technique with low false alarm probability, but it cannot detect the websites that are not in the blacklist database. Because the life cycle of phishing websites is too short and the establishment of blacklist has a long lag time, the accuracy of blacklist is not too high [1].Heuristic-based anti-phishing technique, with a high probability of false and failed alarm, and it is easy for the attacker to use technical means to avoid the heuristic characteristics detection [2]. Similarity assessment based technique is time-consuming. It needs too long time to calculate a pair of pages, so using the method to detect phishing websites on the client terminal is not suitable. And there is low accuracy rate for this method depends on many factors, such as the text, images, and similarity measurement technique [2]. However, this technique (in particular, image similarity identification technique) is not perfect enough yet.

II. REVIEW OF LITERATURE

Phishing attacks can be made online through a variety of means including URL, like fake web pages, Emails, and obfuscation of target web sites, VIRUS and so on. Many techniques came into existence to prevent phishing attacks. One of such method is "Phish-Net: Predictive Blacklisting" to Detect Phishing Attacks; which gathers the information of phishing site from the phish-tank and keep the system secured from such sites [1]. After words "Safe Internet Browsing Using Heuristic Based Technique" but it has high probability of false positives, it was time consuming to use similarity based approaches [2]. Later on "Visual and Textual Content based Anti-Phishing" came in whichVisual based and content based anti-phishing both are widely used anti-phishing techniques. In visual based technique the site

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

is detected by comparing the similarities between the web pages and it detect site is phish or no [3]. After "Security of online electronic transaction" is came in which Secure electronic transaction (SET) is a significant e-commerce protocol designed to improve the security of online transaction [4]. Then the "Online secure payment system using captcha and visual cryptography" the generation of two shares with the help of Visual Cryptography. For authentication of user the system first generates OTP and then OTP is converted into Captcha [5]. In the "Survey paper on Captcha and VRP" a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on the basis of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is a difficult combination of Captcha and a graphical password style [6].After the" Detecting Phishing Websites, a Heuristic Approach" in this paper use a combination of blacklist and a number of heuristic features to determine the legitimacy of the URL [7].

III. PROPOSED SYSTEM

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites. In this 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.

(2, 2)- Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid.
(n, n) -Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image be revealed.
(k, n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.
The proposed methodology has two phases. They are known as registration and authentication. Proposing such system online transaction which deals mainly with monetary or confidential information will be secured.

As shown below in Figure 1 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. 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 are 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 Figure 1.

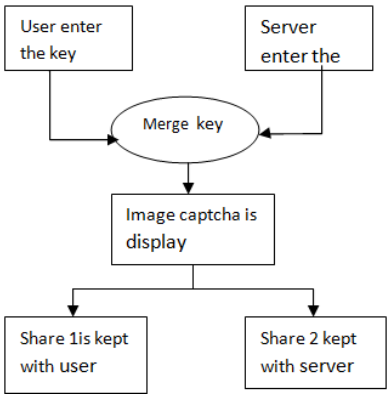


Figure 1: Registration Phase

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

As can be seen below in Figure 2 the Login phase first the user is prompted for the 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. Figure 2 can be used to illustrate the Authentication phase.

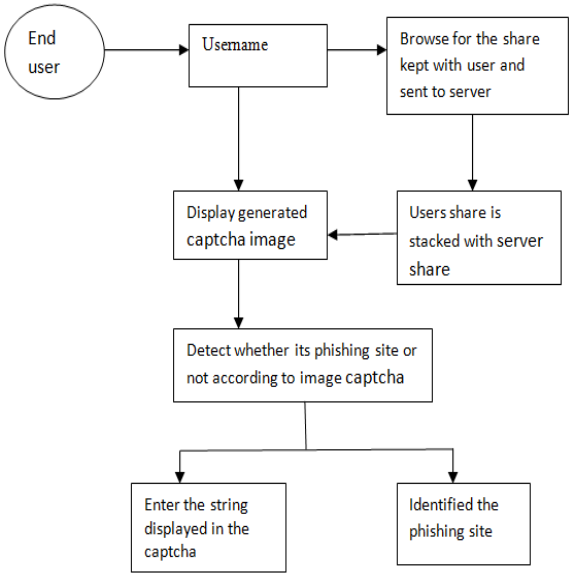


Figure 2: Authentication Phase

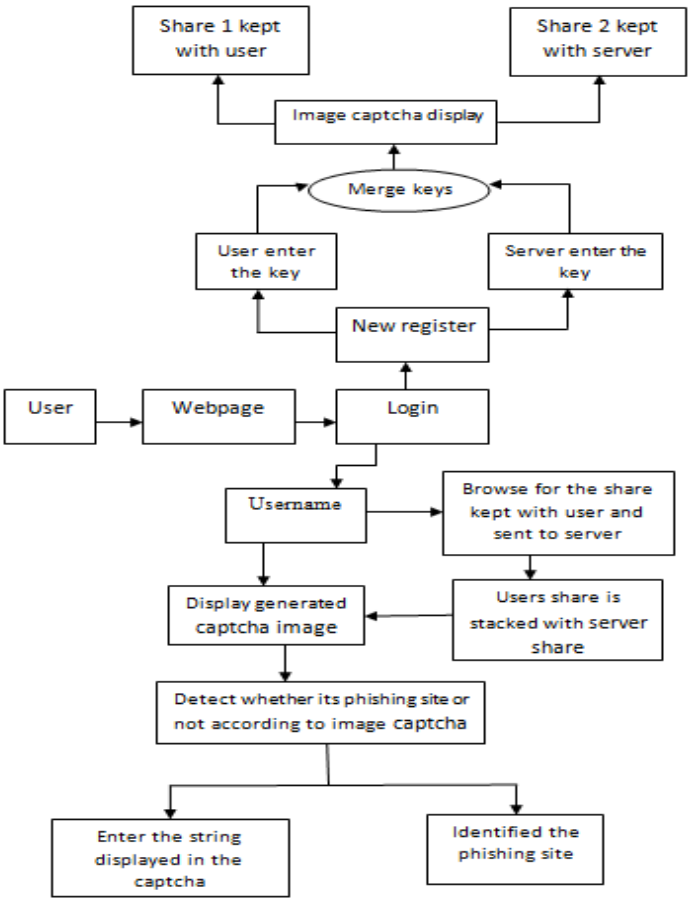


Figure 3: Block diagram

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

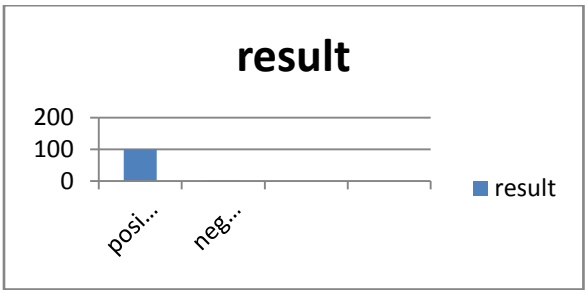
IV. RESULT

The experiments are made generating various captcha images. The proposed technique is used to enhance security for web application to secure the system from phishing attacks whenever the test is carried out.
Experimental results are as presented in the table1

TABLE 1
EXPERIMENT RESULTS

No. Of Experiments	20
Positive Results	20
Negative Results	0

As seen in the table, the system gives 100% result in enhancing the security by generating captcha in secured encrypted form



V. CONCLUSION

Phishing attacks are well known attacks as they can obtain sensitive information from online users. Attackers use such information for monetary benefits. Anti-phishing methodology is nothing but visual cryptography in which image captcha is used to prevent identity theft. When a new user is registered a captcha is associated with the user profile. The captcha image is converted into two shares which are to be kept secret. Only the original user can provide the shares. When both the shares are provided by the user, then only the authentication process gets completed. Thus the proposed system provides complete security to the web site from phishing attacks.
We developed a model net application that demonstrates the proof of thought. The derived results will reveal that the planned anti-phishing theme is effective and may be employed in real time application.

REFERENCES

[1] Pawan Prakash, Manish Kumar, "PhishNet: Predictive Blacklisting to Detect Phishing Attacks" IEEE, 2010
[2] Vibhuti k. Patel, Prof. Hasmukh Patel, "Safe Internet Browsing Using Heuristic Based Technique" international Journal of Engineering Development and Research Volume 2, Issue 2 , 2014
[3] Mr. Digambar Pawar, Mr. Anuraj Jagdale, Mr. Rohit Hinge, Mr. RupeshGangtire, "Visual and Textual Content based Anti-Phishing" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue3, March2016
[4] Nikhil Khandare, Dr. B. B. Meshram , "Security of online electronic transaction" International Journal of Technical Research and Applications Issue 5 ,Nov-Dec 2013
[5] Bittu Kumar, Sumit Brahme, Snehi Suman, Komal Phatak , Prof. A. M. Pawar "Online securepayment system using captcha and visual Cryptography" International Journal of Technical Research Issue 1, Jan 2017
[6] Vijayalaxmi Daundkar, Prashant Kumbharkar" Survey paper on CAPTCHA AND VRP" International Journal of Technical Research Issue 6 November 2015
[7] Suman Bhattacharyya, Chetan kumar Pal, Praveen kumar Pandey" Detecting Phishing Websites, a Heuristic Approach" International Journal of Latest Engineering Research and Applications (IJLERA) Volume–02, Issue –03, March – 2017