An Anti-Phishing Strategy Based on Visual Cryptography

Mrs Bhagyashri Shon Nemane[1], Miss Renu D.Pahurkar[2]

[1,2] *Assistant Professor, Saraswati College Shegaon MS ,India*

Abstract: Phishing is done to acquire confidential information such as usernames, passwords, and credit card details by disguising as a legitimate entity in an electronic communication. In this paper we have proposed a new approach using visual cryptography to solve the problem of phishing. Here an image-based authentication is performed using Visual Cryptography. The image captcha is decomposed into two parts that are stored in separate database servers (one with user and one with server) such that the original image captcha is shown only when both the parts are simultaneously stacked. Once the original image captcha is revealed, the user can use it as the password.

Keywords: Phishing, Visual Cryptography, Image Captcha

1. INTRODUCTION

Online transactions are become very common and important for all human these days and the attacks on this become a very crucial issue. From various types of attacks, phishing is considered as a major security threat. Many new innovative ideas are arising with this concept so preventive mechanisms should also be so effective [3]. Thus the security in these cases be very high and should not be easily tractable with implementation easiness.

Thus, nowadays 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 becomes 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 severe problem for online banking and e-commerce users. The question is how to handle or overcome 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 have been receiving extensive press coverage because such attacks have been increasing rapidly 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”. Another comprehensive definition of phishing, states that it is “the act of sending an email to a user falsely claiming to be an established legitimate enterprise into an attempt to scam the user into surrendering private information that will be used for identity theft”. 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”. So here introduces a new method which can be used as a safe way against phishing which is named as "A novel approach against 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. 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. Visual Cryptography (VC) is a method of encrypting a secret image into shares, such that stacking a sufficient number of shares reveals the secret image.

1.1. Phishing as a Process:

A complete phishing attack involves three roles of phishers:

- Firstly, mailers send out a large number of fraudulent emails (usually through botnets), which direct users to fraudulent websites.
- Secondly, collectors set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information.
- Finally, cashers use the confidential information to achieve a pay-out. Monetary exchanges often occur between those phishers.
- The information flow is shown in Figure 1

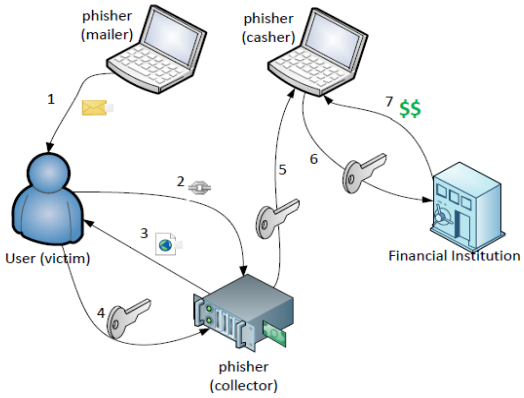

Fig 1: Phishing information flow

1.2. Classification of phishing attack:

Phishing attacks can be classified in to following types according to the way attack is done:

- **Deceptive phishing:**
  In this type of phishing attacker broadcasts an email such as message regarding need to verify account information, re-enter users information because of system failure, undesirable account changes, new free service, and may other scams, with the hope that victim will enter their information and caught in to attackers trap.
- **Malware based phishing:**
  This type of attack involves running malicious software on victims pc, malwares can be introduced as email attachment, or in downloadable file from website, or by exploiting security vulnerabilities.
- **Web Trojans:**
  This kind of attacks pops up invisibly when users attempt to log in. They collect users information locally and transmits to the phisher.
- **System reconfiguration attack:**
  In this type of attack users pc configuration is changed for malicious purpose to redirect users to the URL look alike, for example the Banks URL may be changed from www.gmail.com to www.gmai1.com, we can see here l is replaced by 1.
- **Man in middle phishing:**
  In this type of phishing attacker puts themselves between the user and legal website, they record the user's information and continue to the legal website so that user can not identify, user's transactions are also not affected. Later the sell or use the user's information when user is not active on the system.
- **Search engine phishing:**
  In this type of phishing attacker creates very much attractive website with sound effects, so when users do normal search they find such kind of website and are fooled by giving up their information.

1.3. Target Users:

As expected, targets included social networks, search engines and email services, telecom companies, e-payment services, banks, and other credit and financial institutions. However, there were a few surprises as well, such as tax and customs agencies, the governments of various countries, car companies, insurance companies, medical institutions, oil companies, and transportation companies (including some airlines).

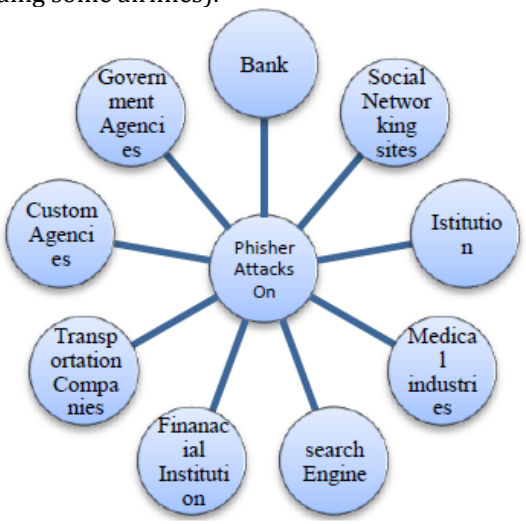

Fig.2: When user performs registration process

2. LITERATURE REVIEW

Liu Wenyin and Anthony Y. Fu[5][6] etc. proposed a page visual similarity assessment method to detect phishing websites, if a web page is similar to a financial organization's page, but it is not the organization's web page itself, it is considered a phishing site's page. JungMin Kang and DoHoon Lee[7] proposed the URL similarity assessment method, if an URL is similar to a bank's URL, but it is not the bank's URL, it is considered a phishing website's URL. There is low assess accuracy rate for the URL and content similarity assessment techniques. The speed of calculating the visual similarity between pages is too slow, so it is only used for phishing-spam detection generally. A three factor authentication scheme named Phish-Secure focuses to counter attack phishing. Here as a first factor of authentication, an image similarity detection

is done which helps in finding out which page the user tends to visit, then it is checked for Phishing .For this purpose a system captures the image of a webpage in a particular resolution in the required format. This image is termed as Visual image. If the attacker is going to create a Phishing site he is going to use the replica of the original webpage in order to fool the users. Now Phish-Secure gets the Visual image of the visited page and collects the mean RGB value of the image. As a second factor of authentication Phish-Secure grabs the destination IP in Layer 3 which gives information about to which IP address the user is getting connected, this is referred as V_IP. If an attacker's web server IP address has already been found guilty the particular IP is blacklisted. Phish-Secure check this Blacklist with the V_IP and will warn the user. An offline phishing detection system named LARX, acronym for Large-scale Anti-phishing by Retrospective data-eXploration to counter phishing attacks has been proposed. First, it uses traffic archiving in a vantage point to collect network trace data. Secondly, LARX leverage cloud computing technology to analyze the experimental data in a way similar to the "divide and conquer" scheme. It used two existing cloud platforms, Amazon Web Services and Eucalyptus. Haijun Zhang, Gang Liu, Tommy W. S. Chow proposed a textual and visual content based antiphishing mechanism using Bayesian approach. This framework synthesizes multiple cues, i.e., textual content and visual content, from the given web page and automatically reports a phishing web page by using a text classifier, an image classifier, and a data fusion process of the classifiers.

3. 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[1].

❖ The proposed approach can be divided into two phases:

A. Registration Phase

B. Login Phase

A. 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. The image CAPTCHA[3][4] 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.3.

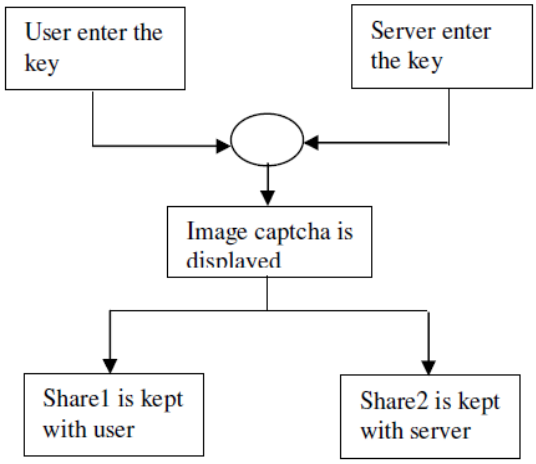

Fig.3: When user performs registration process for the website

B. 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 [1].

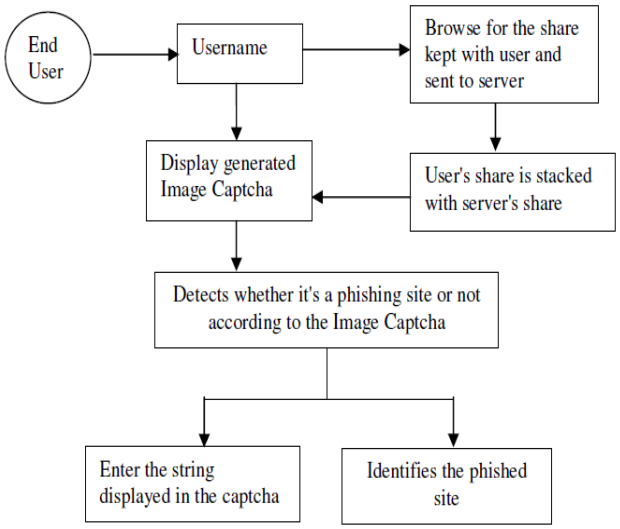

Fig.4: When user performs login process for the website. The overall working scenario can be describe by the following diagram.

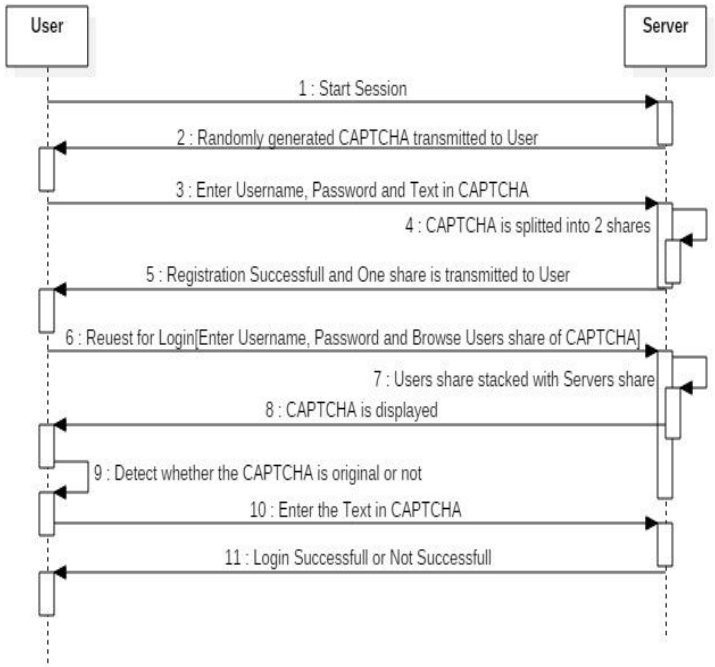

Fig.5: Work flow diagram

5. CONCLUSION

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] Divya James, Mintu Philip, "A novel Anti-phishing framework based on visual cryptography", IEEE 2012
[2] M.Naor and A.Shamir,"Visual cryptography", in Proc. EUROCRYPT, 1994, pp.1-12. IJDPS Vol.3, No.1, 2012.
[3] CAPTCHA: Using Hard AI Problems For Security Luis von Ahn1, Manuel Blum1, Nicholas J. Hopper1, and John Langford.
[4]Mrs. A.Angel Freeda, M.Sindhuja, K.Sujitha, "Image Captcha Based Authentication Using Visual Cryptography".
[5] Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment
Based on Earth Mover's Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3,n 4, p301-311, October/December 2006
[6] Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu, "An Antiphishing Strategy Based
on Visual Similarity Assessment", IEEE Internet Computing, v 10, n 2, p 58-65, March/April 2006.
[7] JungMin Kang, DoHoon Lee, "Advanced White List Approach for Preventing Access to Phishing
Sites", 2007 International Conference on Convergence Information Technology, ICCIT 2007, p 491-496,
2007