ISSN 2395-1621

Phishing Detection Using Visual Cryptography

[#1]Ramiz Khan, [#2]Swapnil Jagtap, [#3]Snehal Shinde, [#4]Amrut Gupta

[#123]Department of Computer Engineering, Flora Institute of Technology, Savitribai Phule Pune University, Maharashtra, India

ABSTRACT

With the advent of internet, various online attacks have been increased and among them the most popular attacks phishing. Phishing is an attempt by an individual or a group to get personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Fake websites which appear very similar to the original ones are being hosted to achieve this. In this paper a new approach named as "An Anti-phishing framework based on visual cryptography "to solve the problem of phishing. Here an image based authentication using Visual Cryptography is implemented. The use of visual cryptography is explored to preserve the privacy of an image captcha by decomposing the original image captcha into two shares (known as sheets) that are stored in separate database servers (one with user and one with server) such that the original image captcha 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. Using this website cross verifies its identity and proves that it is a genuine website before the end users.

ARTICLE INFO

Article History

Received 21st March 2016

Received in revised form :

23rd March 2016

Accepted : 25th March 2016

Published online :

28th March 2016

Keywords— Phishing, Visual Cryptography, Image Captcha, Shares, Security.

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 mechanisms 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 one of them in which illegal activities are per forms using different social engineering techniques. Attackers try to acquire important information such as password, credit card details and confidential data. Definition of phishing state that

Phishing is the fraud method in which sensitive information is acquired by masquerading as a trustworthy for his/her economic or individual gain. Communication channels such as websites, e-mails and instant messaging services are very popular so in these cases, phisher can easily thieve information of authorised users. So to avoid such scenario we need to overcome two problems. First one is to identify whether the site is phishing site or not and second problem is to identify whether the user is authorised or not.One of the best known techniques to protect data is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. The visual cryptography scheme (VCS) is a simple and secure way to allow the secret sharing of images without any cryptographic computations.

II. LITERATURE SURVEY

To scam the victims and to evolve with the anti-phishing techniques, most phishers use more sophisticated and complicated methods to generate the phishing Web page which is similar or even identical to the target Web page and is thus very hard to detect. For example, the phisher can use the screenshot of the target. Web page to directly construct the phishing web page. If the keywords based phishing detection is adopted, this phishing webpage cannot be successfully detected because there are no corresponding keywords directly in the phishing webpage. Phishers sometimes build phishing Web pages purely made up of images, leaving the Cantina no text to analyze, and the text-based technique is infeasible.Though they state that the sheer fact that there are only a bunch of images and a login form without text at all on a web page is a good indicator of a phishing attack, and we could train models using this as a feature, some more complicated designs can also be added to combat this rule, such as adding some HTML sentences with some garbage texts that do not show anything in the generated WebPages. The visual similarity based methods detect phishing attacks by comparing the visual features extracted from the phishing Web page image and the target Web page image, and can effectively deal with these more sophisticated phishing attacks. There are several anti-phishing works based on visual similarity that can seen in this literature.

TABLE I. LITERATURE SURVEY

Techniques	Advantages	Drawbacks
1. Identity Based	Mutual authentication for server as well as client side.	Hacker puts themselves between the user and legal website and can record the user's information.
2. DNS Based	It is most commonly used technique within web browser and easy to implement.	It is ineffective because there is always a chance of vulnerability during which users are susceptible to attacks.
3.Heuristic Based	It provides an efficient checking mechanism where hostname, URL, images are checked to detect phishing.	It has high probability of false alarm, and it's easy for an attacker to use technical means to avoid the heuristic detection.
4. Content Based	It is greater to detection using white and black lists because it does not require the maintenance of lists.	It is insufficient and causes a high rate of false positives.
5.Attribute Based	It considers a lot of checks so it is able to detect more phished sites than other approaches.	As multiple checks perform to authenticate site this could result in slow response time.

III. EXISTING SYSTEM

Existing system include the techniques such as installation of key logger, screen capture, man in the middle attacks, tricking customers through e-mails and spam messages. To avoid this attacks existing technique like One Time Passwords, Personal Identification Number, text captcha can be used. But by using these existing techniques we are not able to analyse the phishing site and 100 percent accuracy is not reserved.

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. 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. 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.

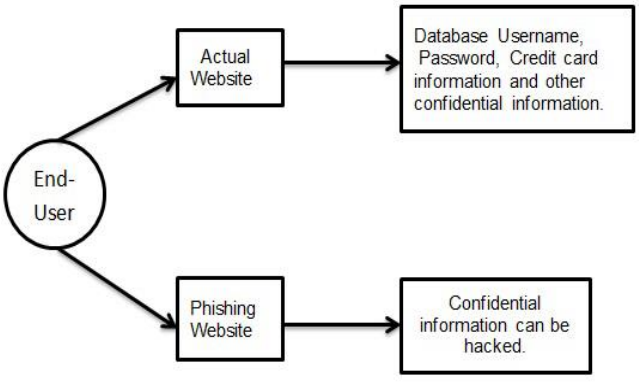

FIGURE I. CURRENT SCENARIO

IV. PROPOSED SYSTEM

For phishing detection and prevention, this paper proposes a new methodology to detect the phishing website. This methodology is based on the Anti-Phishing Image validation scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.

The proposed approach can be divided into two phases:
1. Registration Phase
2. Login Phase

1. Registration Phase

To do any online transaction one need to register to any bank which provide online banking. In this phase user registration is done with the help of Visual Cryptography Algorithm. While registration of user with visual cryptography user is provided by the random images that server have. Among these images user select one image for visual cryptography. The selected image needs to remember by the user which is needed in future. After the selection of image Visual Cryptography algorithm is applied on that image. Output of this phase will give two shares. Out of which first share goes under the process of phase two. And second share will recorded to server side with user id and original image.

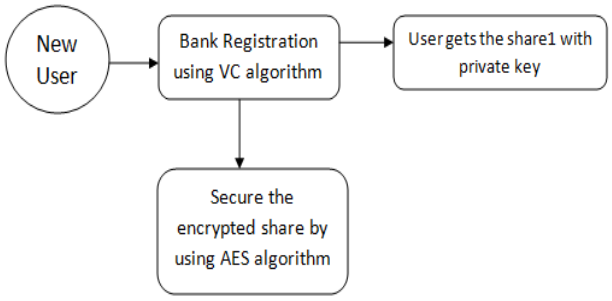

FIGURE II. REGISTRATION PROCESS

2. 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. The image is displayed to the user. Here the end user can check whether the displayed image matches with the image created at the time of registration. The end user is required to enter the text displayed in the image and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image 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.

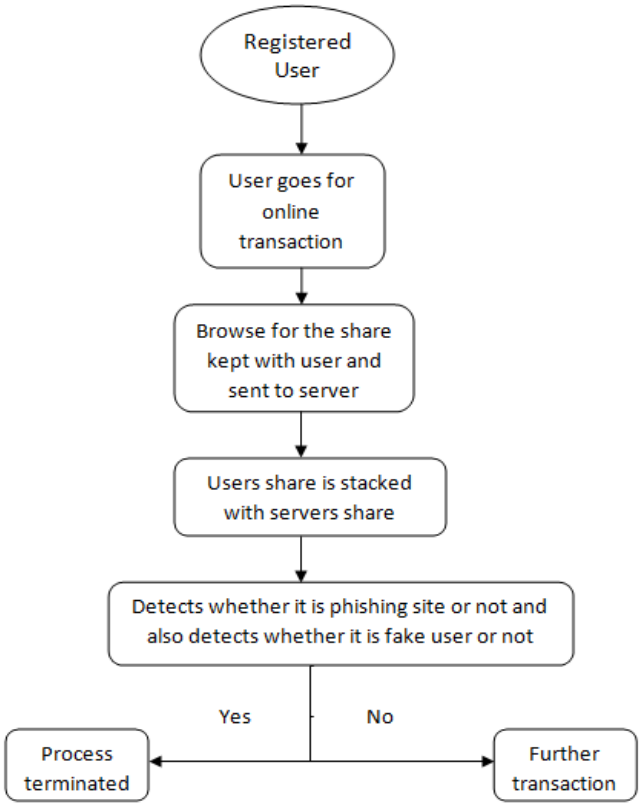

FIGURE III. LOGIN PROCESS

V. SYSTEM ARCHITECTURE

There is a need to give share one to user with secure approach. For that we assign the private key to the encrypted image. And store the private key to server side. When user goes for any transaction need to upload the share one and to authenticate himself, he need to give that private key. By this phase server can be easily identified. When user goes for a transaction, user need to upload the share one. After uploading, server will request for private key. User need to provide private key assigned during registration (in phase two). Now server is with share one and private key. Then server identify the user from that key. Now server stacks its share two with users share one by Visual Cryptography. A new image is formed from these two images. Server will check that image with the original one while user also checks formed image with original image selected in phase one. If formed image is same as original image then proceed further transaction and if it is not phishing is detected and user can terminates the transaction without any loss of confidential data. Image formed and original image is related with the high degree of correlation. But by using Visual Cryptography Algorithm we get very low correlation coefficient. It is observed that by this method obtained correlation coefficient which can be negligible. Hence this shows that there will be zero degree of correlation between original and output images for two different shares.

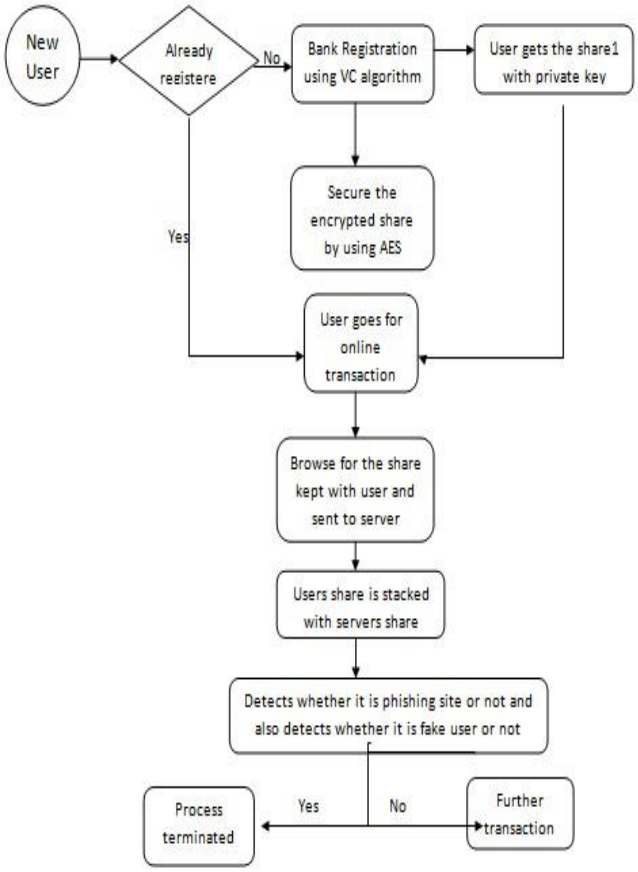

FIGURE IV. SYSTEM ARCHITECTURE

VI. 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 "An Anti-phishing framework based on Visual Cryptography". The proposed methodology preserves confidential information of users using 3 layers of security. First 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).Second layer cross validates image corresponding to the user. The image is readable by human users alone and not by machine users. And as a third layer of security it prevents intruders attacks on the users 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.

ACKNOWLEDGEMENT

We are very grateful to all authors in reference section. Their methods, algorithms, conceptual techniques are very helpful for our research. All papers in the reference section are very useful for our proposed system.

REFERENCES

[1] K.A. Aravind, R. Muthu Venkata Krishnan, Anti-phishing framework for banking based on visual cryptography, IJCSMA, Jan 2014.

[2] Y. YesuJyothi, D.Srinivas, K.govindaraju, The secured anti phishing approach using image based validation, IJRCCT, Sept 2013.

[3] N.Askari, H.M. Heys and C.R. Moloney, An extended visual cryptography scheme for halftone images, 2013 26th IEEE CCECE, 6/13/2013.

[4] Mounika Reddy.M and Madhura Vani.B, A novel anti phishing framework based on Visual cryptography, IJARCCE, Sept 2013.

[5] Divyajames and Mintu Philip, A novel anti phishing framework based on Visual cryptography, 8/12/2012 IEEE.

[6] Tianyang Li, Fuye Han, Shuai Ding and Zhen Chen. "LARX: Large-scale Anti-phishing by Retrospective Data- xploring Based on a Cloud Computing Platform", in Proceedings of IEEE- 20th International Conference on Computer Communications and Networks, 2011.

[7] Thiyagarajan, P. Venkatesan, V.P. Aghila. "Anti-phishing Technique using Automated Challenge Response Method'", in Proceedings of IEEE International Conference on Communications and Computational Intelligience, 2010.

[8] B. Borchert, Segment Based Visual Cryptography, WSI Press, Germany, 2007.

[9] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, An Innocuous Visual Cryptography Scheme, in Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.

[10] T. Monoth and A. P. Babu, Recursive Visual Cryptography Using Random Basis Column Pixel Expansion, in Proceedings of IEEE International Conference on Information Technology, 2007.

[11] The Phishing Guide Understanding and Preventing Phishing Attacks, NGS Software Insight Security Research, 2005.

[12] W.Q. Yan, D. Jin and M. S. Kanakanahalli, Visual Cryptography for Print and Scan Applications, IEEE Transactions, ISCAS-2004.

