A Novel Antiphishing FrameWork on Cloud Based on Visual Cryptography

TusharRaveker , ShreyasSiddh, RizwanShaikh,SanketSugaonkar,Prof. S.S. Vanjire
Sinhgad Academy of Engineering, Pune, Maharashtra, India

ABSTRACT:

Phishing is kind of attack which become popular in recent years . Using phishing attack, attackers can theft the identity of victim by stealing password and other confidential information. Phishing attack mainly used to obtain bank related information which used to gain financial benefits. It has become a serious threat to enterprises that deal with financial transactions. These threats is need to be addressed because increasing used of internet for transactions and banking Many solutions came to solve this kind of identity theft.

To solve the problem of phishing, a framework is proposed based on Visual Cryptography on cloud. In this framework individual can decide whether site is phished or not before entering into sites network. In this framework at the time of registration user enter information, using this information it produces image which is encrypted into two portions that are kept in different database servers (with user and server) such that the original image can be asserted only when both are simultaneously accessible. Once the original image is asserted to the user it can be used for authentication. Hence user can know the site is real or not based on this information. This type of website crosschecks its identity and manifests that it is a legitimate website before the end users.

Keywords:

Share, superposition, grayscale, visualcryptography

INTRODUCTION:

Due to new innovation of new technologies on internet,online transaction and e-purchasing drastically increases. Due to different kind of attack invented in last few years securing the user from attacks is also become crucial in such sites. As the transactions over Internet grow, the possibility of security threats also grows. One of most popular of attack is phishing attack. Thus it is essential to build methodology required to prevent such attacks. Phishing attacks have been recorded in the history in banking and e-commerce domains. This is because these two domains provide monetary transactions online. By stealing identity details of online users one can gain access to original web application and perform activities for which there were not authorized.

Phishing is an attempt to acquire important data assets like username password ATM transaction information by masquerading electronic entity. Phishing is basically used to gain financial gain. In phishing attack attacker can create fake site which is used to gain sensitive information and steal identity of victim which also lead to harassed victim.This system presents a novel method which can be used as a secure path in opposition to phishing which is named as "A novel technique against phishing using visual cryptography". In this approach website crosschecks its own identity and manifests that it is a legitimate website (to use bank transaction, E-

commerce and online booking systems etc.) before the end users and make both the sides of the system safe and authenticated.

In this method ,image processing and visual cryptography is used. Image processing is a method of feed in an image and to get the output as either better form of the original image and/or characteristics of the original image. Visual Cryptography (VC) is a technique of enciphering an image into shares, such that arranging a sufficient number of shares discloses the secret image.

LITERATURE SURVEY:

[1] Ollmann G., "The Phishing Guide Understanding & Preventing Phishing Attacks", NGS Software Insight Security Research, IBM Global Technology Services.

Phishing attacks rely upon a mix of technical deception and social engineering. In most of thecases, the person who wants to do phishing must induce the victim to intentionally perform a series of actions that will provide access to private information. Cryptography is one of the best known techniques to protect. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver.

[2] M. Naor and A. Shamir, "Visual Cryptography," Advances in Cryptolog EUROCRYPT, 1994, Proceeding, LNCS vol. 950, Springer-Verlag, 1995, pp. 1–12.

Introduced the visual cryptography scheme (VCS) as an easy and safe way to allow the secret sharing of images without any cryptographic computations.

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

A segment-based visual cryptography introduced by Borchert can be used only to encrypt the messages containing symbols, especially numbers as bank account number, amount, etc.

[4] W-Q Yan, D. Jin and M. S. Kanakanahalli, "Visual Cryptography for Print and Scan Applications", IEEE Transactions, ISCAS-2004, pp.572-575.

The VCS proposed by Wei Yan et al., can be applied only for printed text or image. He considered the difficulty of precise alignment of printed and scanned visual cryptography shares.

[5] 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, pp. 41-43.

A recursive Visual Cryptography method proposed by Monoth et al., is computationally complex as the encrypted shares are further encrypted into number of sub-shares recursively.

[6] C. M. Hu and W. G. Tzeng, "Cheating Prevention in Visual Cryptography", IEEE Transaction on Image Processing, vol. 16, no. 1, Jan-2007, pp.36-45.

Most of the earlier research work on VC focused on improving two parameters: pixel expansion and contrast. In these cases all participants who hold shares are assumed to be truthful, that is, they will not serve false or fake shares during the phase of recovering the secret image. Thus, the image exhibited on the stacking of shares is considered as the original secrete image. But, thismay not be correct at all times. So dishonesty avoidance techniques are introduced by Hu et al., but, it is observed in all these techniques, there is no provision of authentication test.

[7] S. S. Hegde, BhaskarRao, "Cloud Security Using Visual Cryptography", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012,pp.9-13.

BhaskaraRao et al., proposed a method of providing cloud security by using Visual Cryptography. This scheme provides data access security.

[8] Sian-Jheng Lin and Wei-Ho Chung, "A Probabilistic Model of (t,n) Visual Cryptography Scheme With Dynamic Group", IEEE Transactions on Information Forensics and Security, vol. 7, No. 1, February 2012, pp.197-207.

Sian-Jheng Lin and Wei-Ho Chung et al., proposed a scheme for the (t,n) visual cryptography (VC) is a secret sharing scheme where a secret image is encoded into n transparencies andthe stacking of any out of transparencies reveals the secret image. The stacking of less than t transparencies is unable to extract any information about the secret. So according to this study, We need an approach that can be used as a safe way against phishing which must cross verify website its own identity and proves that it is a genuine website.

EXISTING METHODOLOGY:

In the current scenario as shown in the Fig.1, when the user wants to access his sensitive information online by logging into his account, the user enters information like username and password on the login page. But this information can be stolen by attackers using phishing techniques (for instance, a phishing website can gather the login information the user enters andredirect him to the real site). There is no such information that cannot be directly acquired from the user at the time of his login input.

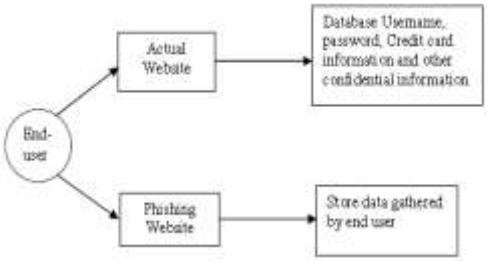

Fig.1:Current Scenario

PROPOSED METHODOLOGY:

For phishing detection and avoidance, we are proposing a new methodology to detect the phishing website. Our methodology is based on the image validation system using visual cryptography. It avoids password and other critical information from the phishing websites.The proposed approach can be divided into two phases:

A. Registration Phase:

In the registration phase, user have to entered information and password. Then server will convert this information into image. This image is divided into two shares. One of the shares is kept on the users cloud account which is created by server for a particular user. The share which is to be stored on the server is again divided into four shares and stored onto the server cloud along with replica for increasing the availability and security.

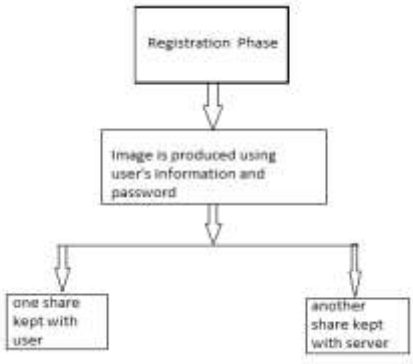

Fig. 2: Registration Phase

B. Login Phase:

In 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. 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. Using the username and image generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website. Figure.3 can be used to illustrate the login phase.

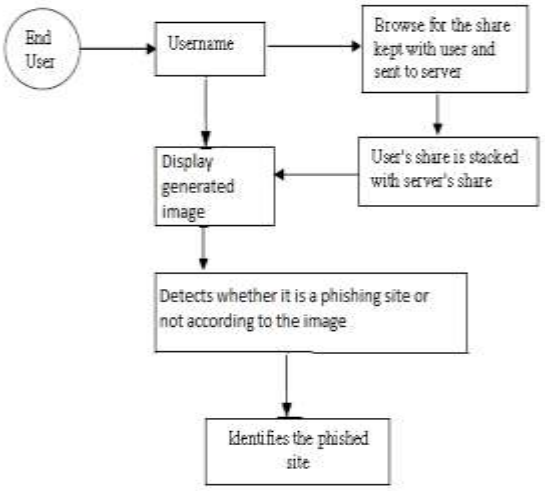

Fig. 3: Login Phase

Second layer cross verifies image CAPTCHA corresponding to the user. The image CAPTCHA is easy to read by human users alone and not by machine users. Only humans accessing the website can read the image CAPTCHA and make sure that the site as well as the user is permitted one or not. So, using image CAPTCHA method, no machine based user can break the password or other critical information of the users. The proposed methodology is also useful to stop the attacks of phishing websites on financial web portal, online shopping market.

ADVANTAGES:

1. High level of security.

2. Protect confidential and private information

3. In this approach website crosschecks its own identity and manifests that it is a legitimate website before the end users and make both the sides of the system safe and authenticated.

4. Helping users to Detects whether it's a phishing site or not according to the Image.

APPLICATIONS:

1. Useful in E-commerce and online booking systems.

2. Useful in bank Web site where bank transaction are done.

3. Useful in Government and Military websites where we want more security.

CONCLUSION:

Currently, phishing attacks are so common because it can attack globally and capture the users' critical information. This critical information is used by the attackers who are indirectly involved in the phishing. Phishing websites can be easily spotted **using our proposed system. The proposed** methodology preserves critical information of users using 2 stages of security. First stage confirms whether the website is a genuine website or a

phishing website. If a website is a phishing then in that circumstance, the phishing website can't show the original image for that particular user because the original image is generated by the stacking of two shares, one with the user and another with the real database of the website. Second layer cross verifies image CAPTCHA corresponding to the user. The image CAPTCHA is easy to read by human users alone and not by machine users. Only humans accessing the website can read the image CAPTCHA and make sure that the site as well as the user is permitted one or not. So, using image CAPTCHA method, no machine based user can break the password or other critical information of the users. The proposed methodology is also useful to stop the attacks of phishing websites on financial web portal, online shopping market.

ACKNOWLEDGEMENT:

We sincerely thank to all authors in reference section. All papers in reference section are very useful for our proposal. We would like to thank Prof. S.S.VANJIRE for her comments and our friends for reviewing this paper and providing their useful and constructive comments.

REFERENCES:

[1] Ollmann G., "The Phishing Guide Understanding & Preventing Phishing Attacks", NGS Software Insight Security Research, IBM Global Technology Services.

[2] M. Naor and A. Shamir, "Visual Cryptography," Advances in Cryptology EUROCRYPT, 1994, Proceeding, LNCS vol. 950, Springer-Verlag, 1995, pp. 1–12.

[3] G. R. Blakley, "Safeguarding Cryptographic Keys", Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.

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

[5] W-Q Yan, D. Jin and M. S. Kanakanahalli, "Visual Cryptography for Print and Scan Applications", IEEE Transactions, ISCAS-2004, pp.572-575.

[6] 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, pp. 41-43.

[7] C. Blundo and A. De Santis, "On the contrast in Visual Cryptography Schemes", In Journal on Cryptography, vol. 12, 1999, pp. 261-289.

[8] C. M. Hu and W. G. Tzeng, "Cheating Prevention in Visual Cryptography", IEEE Transaction on Image Processing, vol. 16, no. 1, Jan-2007, pp.36-45.

[9] S. S. Hegde, BhaskarRao, "Cloud Security Using Visual Cryptography", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012,pp.9-13.

[10] Sian-Jheng Lin and Wei-Ho Chung, "A Probabilistic Model of (t,n) Visual Cryptography Scheme With Dynamic Group", IEEE Transactions on Information Forensics and Security, vol. 7, No. 1, February 2012, pp.197-207.