K.A.Aravind *et al*, International Journal of Computer Science and Mobile Applications,

Vol.2 Issue. 1, January- 2014, pg. 121-126 **ISSN: 2321-8363**

Anti-Phishing Framework for Banking Based on Visual Cryptography

Mr.K.A.Aravind[1], Mr.R.MuthuVenkataKrishnan[2]

[1]PG Student, [2]Assistant Professor, Department of Computer Science and Engineering,

PRIST University, Chennai Campus, Tamilnadu, India

([1] aravind68@live.com)

Abstract

Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc from unsuspecting victims for individuality theft, economic gain and other fake activities. In this thesis we have projected a new loom named as "A Novel Antiphishing framework based on visual cryptography" to solve the difficulty of phishing. Here an picture base verification by means of Visual Cryptography (vc) is used. The exploit of visual cryptography is explore to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers 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 picture captcha. Once the unique picture captcha is discovered to the user it can be used as the password.

Index Terms — Phishing attack, visual cryptography, Image processing, Image captcha generation.

I. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks here after this. In this type of different attack, phishing is known as a foremost protection threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so efficient. Thus the safety in these cases be awfully high and should not be easily tractable with execution acceptance. Nowadays, the majority of the application is only as protected as their primary system. Since the propose and expertise of middleware has enhanced gradually, their detection is a complex problem. As a result, it is nearly not possible to be sure whether a processor that is linked to the internet can be considered trustworthy and secure or not. Phishing scam is also becoming a hitch for online banking and e-commerce users. The query is how to hold applications that require a high point of security. Phishing is a form of online individuality stealing that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication.

One definition of phishing is specified as “it is a illegal activity using social engineering techniques. Phishers try to falsely acquire susceptible information, such as passwords and credit card details, by hidden as a trustworthy person

or business in an electronic communication". Another complete definition of phishing, states that it is "the act of transfer an email to a user falsely claim to be an establish legal enterprise into an attempt to scam the user into yielding personal information that will be used for self theft". The conduct of identity theft with this acquire receptive information has also become easier with the use of technology and identity theft can be describe as "a crime in which the fake obtains key pieces of information such as Social Security and driver's license information and uses them for his or her own grow". Phishing [1] attacks rely upon a combine of technological deception and social engineering practices. In the majority of cases the phisher must convince the victim to purposely perform a series of actions that will provide access to secret information. Communication channels such as email, web pages, IRC and instant messaging services are popular. In all cases the phisher must imitate a trusted source (e.g. the helpdesk of their bank, automated support response from their favorite online retailer, etc.) for the victim to consider. To date, the most triumphant phishing attacks have been initiate by email – where the phisher impersonate the sending authority (e.g. spoofing the source email address and embedding appropriate corporate logos). For example, the victim receives an email supposedly from support@mybank.com (address is spoofed) with the subject line 'security update', requesting them to follow the URL www.mybank-validate.info (a domain name that belongs to the attacker – not the bank) and offer their banking PIN number. So here introduce a new way which can be used as a safe method 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 authentic website (to use bank transaction, E-commerce and online booking system etc.) prior to the end users and make the both the sides of the system secure as well as an valid one. The concept of image processing and an enhanced visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either better form of the same image and/or characteristics of the input image. Visual Cryptography (VC) is a method of encrypting a secret image to shares, such that stacking a enough number of shares reveals the secret image.

II. RELATED WORK

2.1 Project overview

Phishing web pages are fake web page that is created by wicked people to imitate Web pages of actual web sites. These pages are typically having high visual similarity to trick their sufferers. To overcome this difficulty concept of image processing and an enhanced visual cryptography is used. Image processing is a method of processing an input image and to get the output as either better form of the same image and/or characteristics of the input image. VCS is a cryptographic procedure that allow for the encryption and decryption of visual information. The use of visual cryptography is explore to protect the privacy of image captcha by decomposing the original image captcha into two shares that are stored in various database servers such that the original image captcha can be exposed only when both are concurrently available.

2.1.1 Scope of project

- Main scope of this project is to protect the online users from phishing sites using visual cryptography.
- Anti phishing framework based on visual cryptography to solve the problem of phishing.
- Image based authentication using Visual Cryptography (VC) is used.
- Visual Cryptography is used to decompose an image into shares.
- Original image is revealed by combining the appropriate image shares.
- Finally it helps in preventing the password and other confidential information from the phishing websites.

Vol.2 Issue. 1, January- 2014, pg. 121-126 **ISSN: 2321-8363**

2.2 Existing System

Phishing web pages are fake web pages that are created by wicked people to imitate Web pages of real web sites. Most of these kind of web pages have high visual similarity to trick their sufferers. Some of these kinds of web pages look precisely like the real ones. Victims of phishing web pages may represent their bank account, password, credit card number, or other vital information to the phishing web page owners. It includes technique such as tricking customers through email and spam messages, man in the middle attacks, installation of key loggers and screen capture.

2.2.1 Disadvantages

- Accuracy of blacklist is not too high.
- Heuristic-based anti-phishing technique, with a high probability of false and failed alarm.
- Similarity assessment based technique is time-consuming.

2.3 Proposed system

The theory of image processing and an enhanced visual cryptography is used. Image processing is a method of processing an input image and to get the output as either better 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 expose the original image proper number of shares should be shared. VCS is a cryptographic method that allows for the encryption of visual information such that decryption can be performed using the human visual system.

2.4 SYSTEM ARCHITECTURE

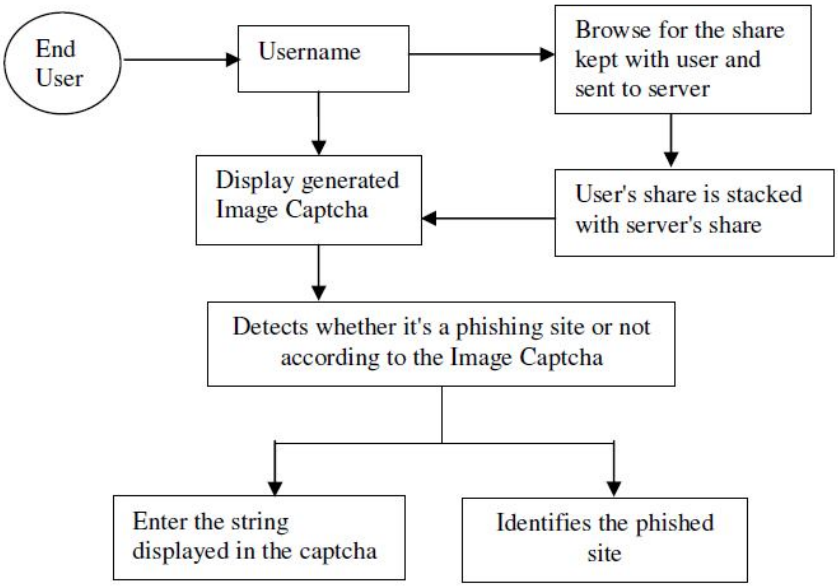

Fig 1 System Architecture Diagram

2.5 DATA FLOW DIAGRAM

2.5.1 LEVEL 0

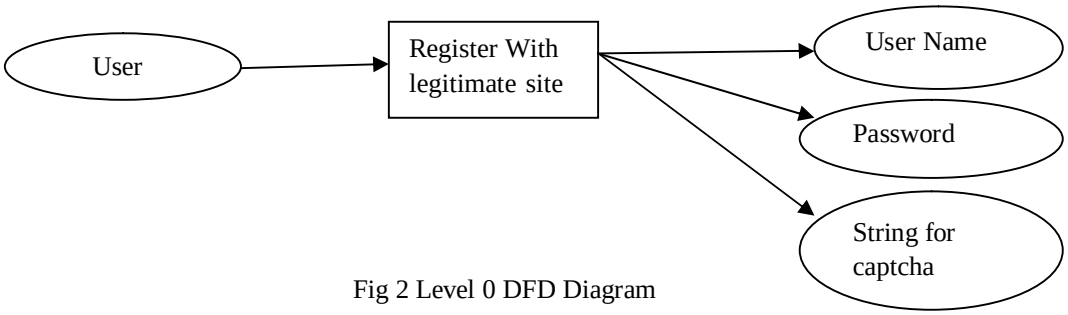

Fig 2 Level 0 DFD Diagram

2.5.2 LEVEL 1

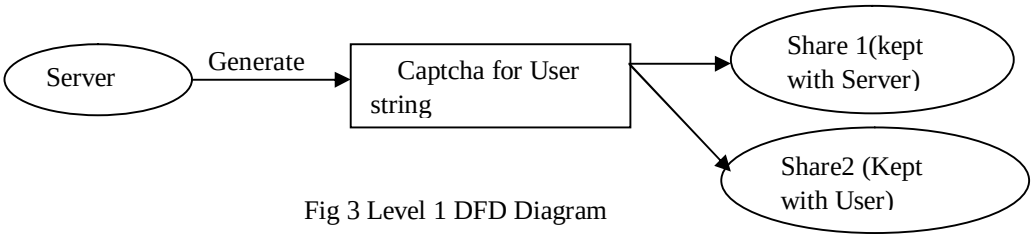

Fig 3 Level 1 DFD Diagram

2.5.3 LEVEL 2

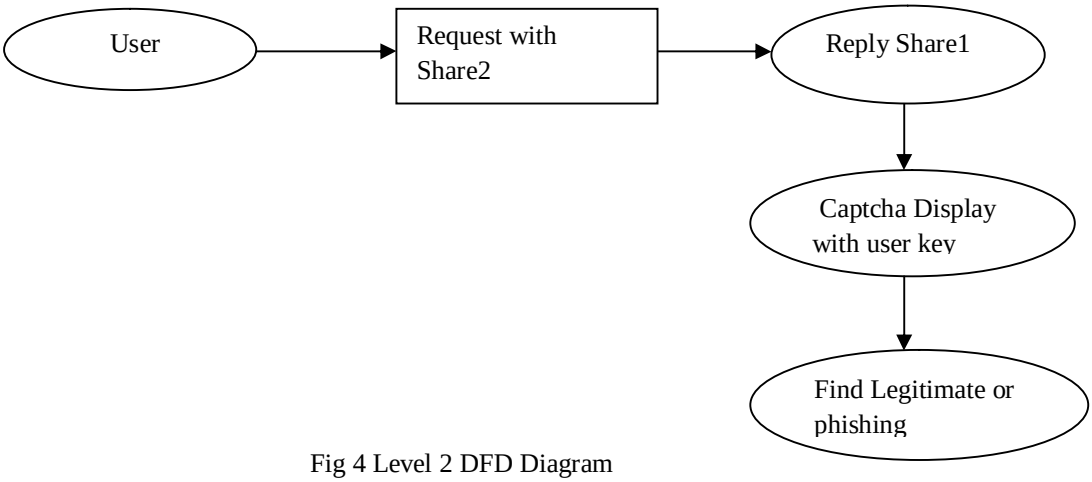

Fig 4 Level 2 DFD Diagram

Vol.2 Issue. 1, January- 2014, pg. 121-126 **ISSN: 2321-8363**

III. ALGORITHM AND TECHNIQUE

Grayscale conversion:

The captcha image first converts into grayscale using luminance method.

Luminosity:

The gray level will be calculated as
Luminosity = 0.21 × R + 0.72 × G + 0.07 × B

Vcs scheme:

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 shares provide 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.

IV. CONCLUSION

At present phishing attacks are so common because it can attack worldwide and capture and store the users' secret information. This information is used by the attacker which is not directly involved in the phishing process. Phishing websites as well as human users can be simply known using our proposed "Anti-phishing framework based on Visual Cryptography". The proposed method preserves secret information of users. 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 related to secure website but not the secure website), then in that state, the phishing website can't display the image captcha for that specific user (who wants to log in into the website) due to the fact that the image captcha is generated by the stacking of two shares, one with the user and the other with the actual database of the website. The proposed methodology is also useful to prevent the attacks of phishing websites on economic web portal, bank portal, online shopping marketplace.

ACKNOWLEDGEMENT

I sincerely thanks to all authors in reference section. All papers in the reference section are very useful for my proposal. Their concepts, algorithms and techniques are very useful for my research.

REFERENCES

[1] Ollmann.G, the Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.
[2] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
[3] A. Shamir, .How to Share a Secret,. Communication ACM, vol. 22, 1979, pp. 612-613.
[4] G. R. Blakley, .Safeguarding Cryptographic Keys,. Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.

[5] A. Menezes, P. Van Oorschot and S. Vanstone, .Handbook of Applied Cryptography,. CRC Press, Boca Raton, FL, 1997.
[6] B. Borchert, .Segment Based Visual Cryptography,. WSI Press, Germany, 2007.

