*IOSR Journal of Computer Science (IOSR-JCE)*
*e-ISSN: 2278-0661, p-ISSN: 2278-8727*
*PP 11-15*
*www.iosrjournals.org*

# A Survey On Efficient Anti Phishing Method Based on Visual Cryptography Using Cloud Technique By Smart Phones

Prasad D. Baitule[1], Swapnil P. Deshpande[2]
[1,2]Computer Engineering, Bapurao Deshmukh College of Engineering / R.T.M Nagpur university, India

***ABSTRACT:****Phishing is nothing but an attempt made by an individual or group to thieve personal confidential information such as password, credit card information, Transaction Number etc. from unsuspecting victims for identity theft and fraudulent activities. Since the importance of smart phones is increased day to day as more applications are deployed and executed. In this paper, a new approach named as "An Efficient Anti phishing method based on Visual Cryptography using cloud technique by smart phones" to solve the problem of phishing. The visual cryptography is explored to preserve the privacy image Captcha by decomposing it into two shares that are stored in cloud (data severs) such that, when original Captcha can be revealed when the both are available at same time. Since users are unable to carry the Captcha place to place so a concept of Image Captcha conversion into String with the help of cloud is revealed which can be used as the password.*

**Keywords:Cloud**,Phishing, String, Share, Security, Smart phones, Visual Cryptography.

## I. INTRODUCTION

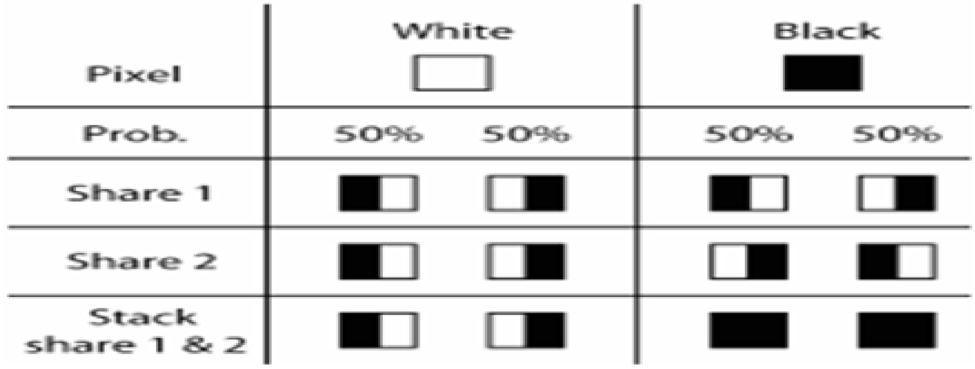
Now-a-days online usages like transactions, Recharges are becoming very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanisms should also be so effective .Thus the security in these cases be very high and should not be easily tractable with implementation ***easiness. 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 device that is connected to the internet can be considered trustworthy or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question arises is how to handle applications that require a high level of security.

### 1.1. Phishing and Anti Phishing

***Phishing*** is the act of attempting to acquire information by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing web pages are forged web pages that are created by malicious people to mimic Web pages of real web sites having high visual similarities to scam their victims. Some of these kinds of web pages look exactly the real ones. ` ***Anti phishing*** refers to the method employed in order to detect and prevent phishing attacks. A lot of work has been done on anti-phishing devising various anti-phishing techniques. Some techniques works on emails, some works on attributes of web sites and some on URL of the websites. Many of these techniques focus on enabling clients to recognize & filter various types of phishing attacks.

### 1.2. Visual Cryptography

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. 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.

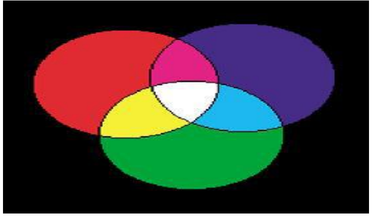


| Pixel | White<br>□ | | Black<br>■ | |
|---|---|---|---|---|
| Prob. | 50% | 50% | 50% | 50% |
| Share 1 | ■□ | □■ | ■□ | □■ |
| Share 2 | ■□ | □■ | □■ | ■□ |
| Stack share 1 & 2 | ■□ | □■ | ■■ | ■■ |

**Fig 1.2 Construction of (2, 2) VC Scheme.**

(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.

***Hou*** shares generated by applying halftone methods and colour decomposition. He decomposed the colour image into three (yellow, magenta and cyan) halftone images and then improvised three coloured 2-out-of-2 VC schemes which follow the subtractive model. Thus in the (C,M,Y) representation (0,0,0) represents full white and (255,255,255) represents full black.



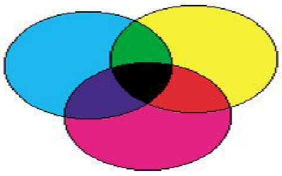


**Fig 1.2.a) Additive Model (R,G,B)** **Fig 1.2.b) Subtractive Model(C,Y,M)**

### 1.2.1 Halftoning

The main idea of halftoning is to utilize the density of printed dots to simulate the grey scale of pixels. For human eyes, the denser the dots are, the darker the image is; on the contrary, the sparser the dots are, the lighter the image is. For example, if the black dot densities of two areas with same size are 90% and 50% respectively, the human visual system can perceive the difference between them: the former is darker than the image provided to human. In general anti-phishing techniques can be classified into following categories.

### 1.3. Cloud Technology

Clouds are a very new and popular topic in the field of IT. Though this is not a new technology, it is a new concept: the main purpose of the original cloud is that “users can use the service anytime, anywhere through the Internet, directly through the browser.” It is an extension of distributed computingthrough the Internet. A huge operation procedure is automatically split into several smaller operation procedures, processed by a number of extensive systems of the server, and the output finally goes through the search and operations to return to the user.Simply by using clouds, users can store personal data and back up actions. The cloud can also be used simply for personal data management and real-time updates. It can be used anytime and anywhere by users with mobile phones as a carrier. The biggest issue with mobile users keeping personal data in the cloud is security of the personal data.Since it is difficult for user to carry the Captcha from place to place so therefore here we revealed the concept of String Conversion using cloud technique. If a user Captcha is tampered or damaged or stored in a device likewise Pen-drive etc. which get lost or damage then the share which is to be opened up by using the share of user and share from server which will not get revealed and thus the information may not be available to the user itself which is major issue related to it. So for increase the usage efficiency and less time consuming towards the user here the concept of cloud for keeping backup of the client and provide it to user whenever needed. For user point the simplest thing is that users need not to carry the Captcha within it, just by using it from cloud accessing as string. This will reduce the consumption time of user Captcha which to be carried when user want to access any Web /emails etc. As the mentioned anti phishing techniques are also utilize within this paper. Here cloud is used for the stored purposed from where users can easily access. In this paper (2,2) Threshold VCS scheme used that takes a secret message and encrypt into different shares that revealthe image when they overlaid. Since this paper covers issues related to Image Captcha, cloud technique and various anti phishing methods.

## II. EXISTING SYSTEM

In the current scenario, when the end user wants to access his confidential information online by logging secure mail or confidential account, the person enters information like username, password, credit card no. etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such information that cannot be directly obtained from the user at the time of his login input.

## III. PROPOSED WORK

### Working description

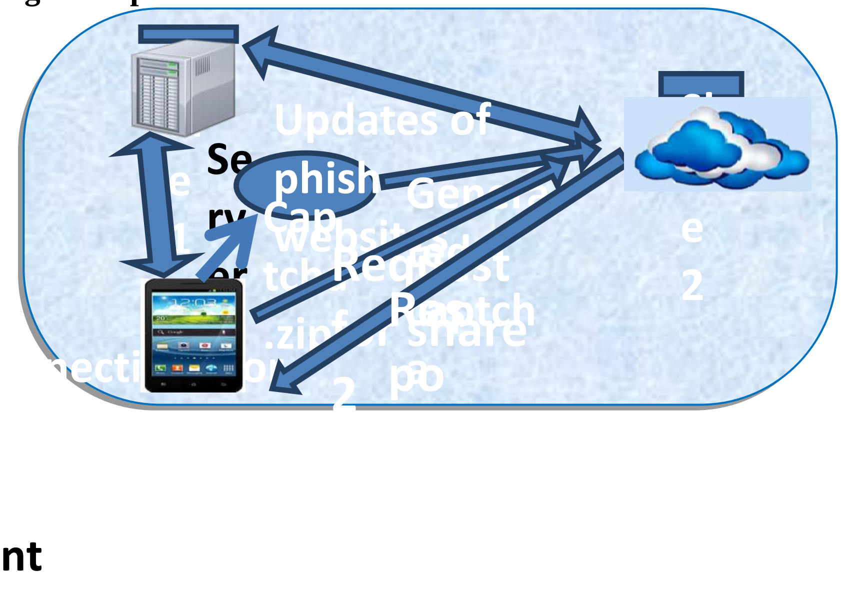


**Fig.** 3 system architecture

The mentioned System Architecture is 3-tier Architecture and consists of client as a Smart phone, server and cloud as for storage to store captcha and security purpose used for developing the application. Each key term in mentioned architecture has its own functionalities having set of activities to perform the targeted task of the paper. Client/server architecture works when the client computer sends a resource or process request to the server over the network connection, which is then processed and delivered to the client. A server computer can manage several clients simultaneously, whereas one client can be connected to several servers at a time, each providing a different set of services

For phishing detection and prevention, the paper has a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography and the concept of cloud for keeping backup of the client and provides it to user whenever needed. For user point the simplest thing is that users need not to carry the Captcha within it, just by using it from cloud accessing as string. This will reduce the consumption time of user Captcha which to be carried when user want to access any Web /emails etc. It prevents password and other confidential information from the phishing websites. The proposed work divided into two phase.

A. Registration phase
B. Login phase

### A. 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 in which the string is made available from the image Captcha 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. Registration process is depicted in Figure

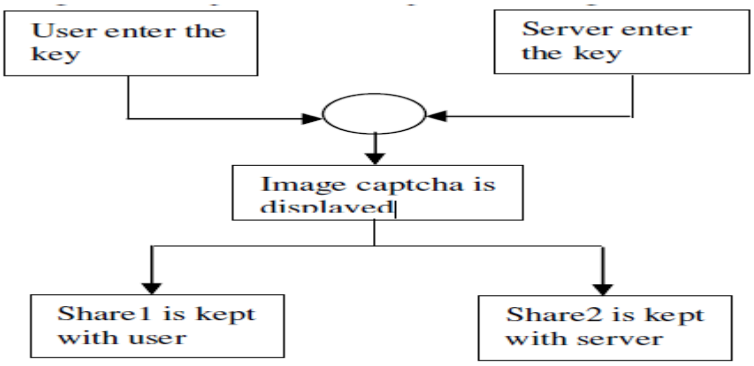


**Fig.** Aregistration process for web sites

### Image Generation

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. 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.

### Captcha Creation converting to string for user

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.

### B. Login phase

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. Figure shown below denotes login.

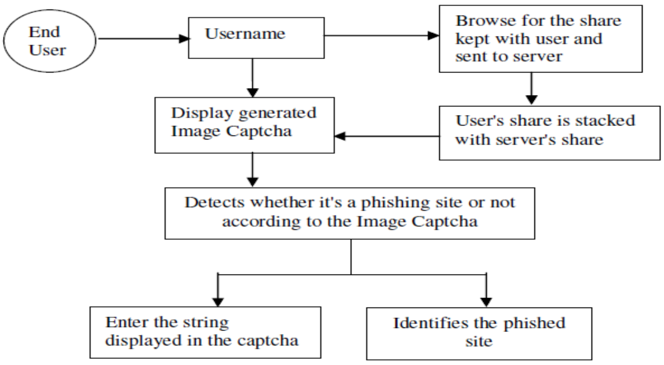

End User
Username
Browse for the share kept with user and sent to server
Display generated Image Captcha
User's share is stacked with server's share
Detects whether it's a phishing site or not according to the Image Captcha
Enter the string displayed in the captcha
Identifies the phished site

**Fig.** B user attempt to login the site

## IV. CONCLUSION

This survey paper preserves confidential information of users. It verifies whether the website is a secure website or a phishing website and also it cross validates image Captcha corresponding to the user. Only users accessing the website can read the Captcha converted into string within cloud and ensure that the site as well as the user is permitted one or not. And it also prevents intruders' attacks on the user's account.

## REFERENCES

[1] Thiyagarajan, P.; Venkatesan, V.P.; Aghila,G.*"Anti-Phishing Technique using Automated Challenge Response Method'"*, in Proceedings of IEEE- International Conference on Communications and Computational Intelligence, *2010.*

[2] Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; *"A DNS based Anti-Phishing Approach,"* in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, *2010*

[3] 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.*

[4] Nirmal, K.; Ewards, S.E.V.; Geetha, K.; *"Maximizing online security by providing a 3 factor authentication system to counter-attack 'Phishing'"*, in Proceedings of IEEE- International Conference on Emerging Trends in Robotics and Communication Technologies, *2010.*

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

[6] M.Naor and A. Shamir, "*Visual cryptography*," in Proc. EUROCRYPT, 1994, pp. 1–12. International Journal of Distributed and Parallel Systems *(IJDPS) Vol.3, No.1, January 2012 218.*

[7] 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.*

[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] *"The NIST Definition of Cloud Computing"*. National Institute of Standards and Technology, *Retrieved 24 July 2011*.[10]. Jaya *"Securing Cloud Data and Cheque Truncation System with Visual Cryptography"* International Journal of Computer Applications *(0975 – 8887) Vol. 70– No.2, May 2013*[11] A Text-Graphics Character CAPTCHA for Password Authentication Matthew Dailey Chanathip Namprempre.