International Journal of Technology and Engineering System (IJTES)
Vol 7. No.2 2015 Pp. 118-123

available at : www.ijcns.com
ISSN: 0976-1345

AUTHENTICATION PROTOCOL FOR SECURITY BASED CAPTCHA AS A COUNTERSIGN ON HARD AI PROBLEMS

S.BANUPRIYA[1] G.SOWMIYA[2] C.KOMALA[3], J.GOBINATH[4,]
[1,2,3]*Bachelor of Engineering, Dept of IT*
, [4]Assistant Professor, Dept of IT
Rajiv Gandhi College of Engineering, Chennai, India
priyabanuapk@gmail.com[1] sowmichala@gmail.com[2]
gobirgce@gmail.com[4]

ABSTRACT

Phishing is an attempt by an individual or a group to thieve personal confidential information. New approach of phishing websites classification is proposed to solve the problem of phishing. Security of trustee based authentications. Phishing websites comprise a variety of cues within its content. Browser-based security indicators provided. Original image CAPTCHA into two shares that are stored in separate database servers. Once the original image CAPTCHA is revealed to user it can be used as the password. Anti-phishing solutions aim to predict the website class accurately and that exactly matches the data mining classification technique goals. The feature of the system is to distinguish phishing websites from legitimate ones and assess. Rule-based data mining classification techniques are in predicting phishing websites. Classification technique is proven to be more reliable.

Index Terms: CAPTCHA, Phishing Websites, Authentication, Data Mining

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 mechanism 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 a form of online identity theft 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 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”. 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”. Phishing attacks rely upon a mix of technical deceit and social engineering practices. Communication channels such as email, web pages, IRC and instant messaging services are popular. In all cases the phishes must impersonate a trusted source for the victim to believe. To date, the most successful phishing attacks have been initiated by email – where the phishes impersonates the sending authority So here they 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 it 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 to shares, such that stacking a sufficient number of shares reveals the secret image.

RELATED WORK

A large number of graphical password schemes have been proposed. They can be classified into three categories according to the task involved in memorizing and entering passwords: recognition, recall, and cued recall. [1].A recognition-based scheme requires identifying among decoys the visual objects belonging to a password portfolio. A typical scheme is Pass faces [2] wherein a user selects a portfolio of faces from a database in creating a password. [3]Captcha relies on the gap of capabilities between humans and bots in solving certain hard AI problems. There are two types of visual text CAPTCHA and Image-Recognition Captcha (IRC). It was introduced in [4] to use both Captcha and password in a user authentication protocol, which we call CaptchabasedPasswordAuthentication (CbPA) protocol, to counter online dictionary attacks. The CbPA-protocol in [5] requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser receives cookie.

Existing System

Phishing web pages are forged web pages that are created by malicious people to mimic Web pages of real web sites. Most of these kinds of web pages have high visual similarities to scam their victims. Some of these kinds of web pages look exactly like the real ones. Victims of phishing web pages may expose their bank account, password, credit card number, or other important information to the phishing web page owners. It includes techniques such as tricking customers through email and spam messages, man in the middle attacks, installation of key loggers and screen captures.

II.SYSTEM DESIGN

System Design involves identification of classes their relationship as well as their collaboration. In objector, classes are divided into entity classes and control classes. The Computer Aided Software Engineering (CASE) tools that are available commercially do not provide any assistance in this transition. CASE tools take advantage of Meta modeling that is helpful only after the construction of the class diagram. In the FUSION method some object-oriented approach likes Object Modeling Technique (OMT), Classes, and Responsibilities. Collaborators (CRC), etc, are used. Objector is used the term “agents” to represent some of the hardware and software system. In Fusion method, there is no requirement phase, where a user will supply the initial requirement document. Any software project worked out by both the analyst and the designer. The analyst creates the user case diagram. The designer creates the class diagram. But the designer can do this only after the analyst creates the use case diagram. Once the design is over, it is essential to decide which software is suitable for the application.

III.PROPOSED SYSTEM

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. It denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides 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. 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.

Random Pattern Algorithm

Random pattern algorithm is to encrypt a binary secret image. The input of the algorithm is a w × h image, denoted by A, and the outputs are two images R1 and R2. One of their algorithms is shown as below.

Generate a w × h random grid R1// $\Im(R1) = ½$

```
for( i = 0 ; i < w ; i ++ )

for (j = 0 ; j < h ; j ++ )

if( A[i][j] == 0 )
```

R2 [i][j] = R1 [i][j] ;

Else

R2 [i][j] = R1 [i][j] ;

Output (R1 , R2)

Based on the above algorithm, this work proposes a new algorithm, process one gray-level secret image, denoted by B, and generates two gray-level encrypted images, denoted by G1 and G2, that all pixels are classified into more than two colors. When user overlaps those two encrypted images G1 and G2, the hidden secrets of the gray-level image B can be shown. According to the range of RGB value in gray-level, two methods below are concluded to encrypt every pixel on the gray-level secret image.

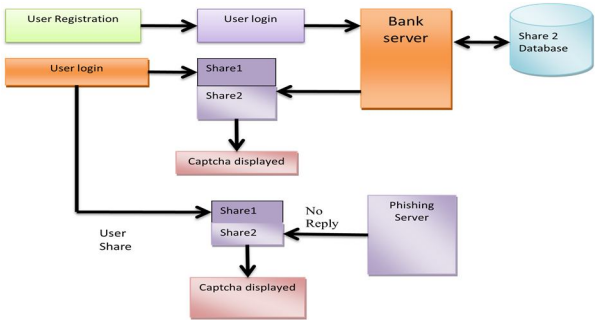

Fig 1.Overall Architecture Diagram

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.

IV.SYSTEM IMPLEMENTATION

Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is workable and effective. It may be implementation of a modified application to replace an existing one. This type of conversation is relatively easy to handle, provide there are no major changes in the system. Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly. Initially as a first step the executable form of the application is to be created and loaded in the common server machine which is accessible to the entire user and the server is to be connected to a network. The final stage is to document the entire system which provides components and the operating procedures of the system. Implementation is the stage of the project when the theoretical design is turned out into a working system.

Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. Implementation is the process of converting a new system design into operation. It is the phase that focuses on user training, site preparation and file conversion for installing a candidate system. The important factor that should be considered here is that the conversion should not disrupt the functioning of the organization

DFD Module

The Data Flow diagram is a graphic tool used for expressing system requirements in a graphical form. The DFD also known as the "bubble chart" has the purpose of clarifying system requirements and identifying major transformations that to become program in system design. Thus DFD can be stated as the starting point of the design phase that functionally decomposes the requirements specifications down to the lowest level of detail. The DFD consist of series of bubbles joined by lines. The bubbles represent data transformations and the lines represent data flows in the system. A DFD describes what that data flow in rather than how they are processed. So it does not depend on hardware, software, data structure.

DATA FLOW DIAGRAM

LEVEL 0:

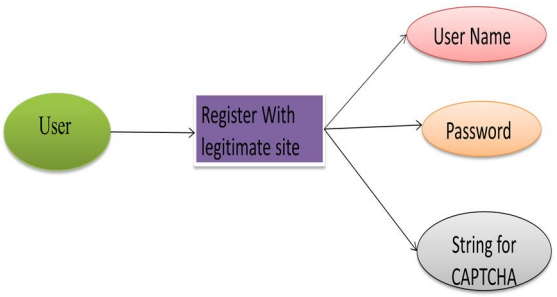

Fig 2 .Registration in Legitimate Site

LEVEL 1:

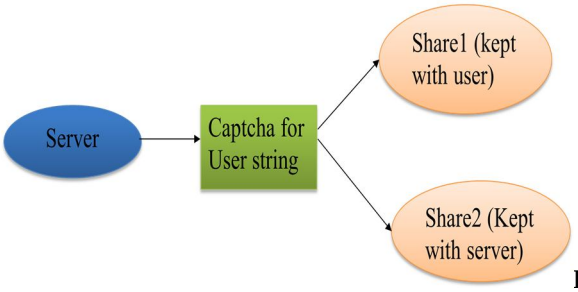

Fig 3.Generation of Shares

LEVEL 2:

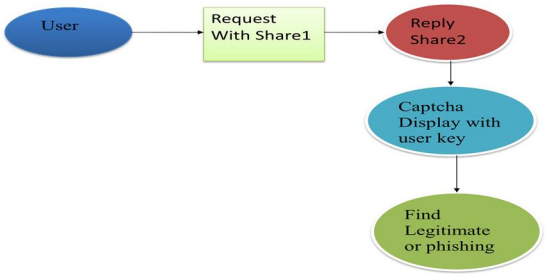

Fig 3.Login Process

V.EVALUATION RESULT

In the registration phase, the user details user name, password, email-id, address, and a key string (password) asked from the user at the time of registration for the secure website.

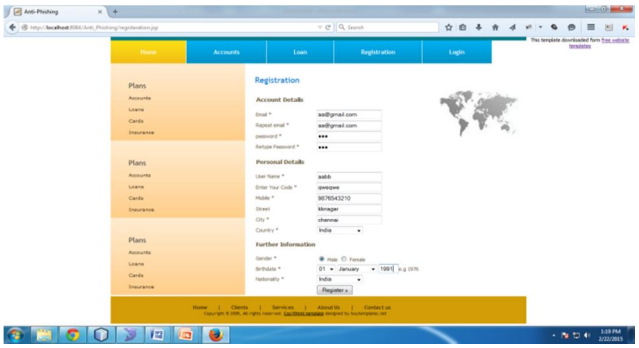

Fig 5.Registration Form

A key string is converted into image using java classes Buffered Image and Graphics2D. The image dimension is 260*60. Text color is red and the back round color is white.

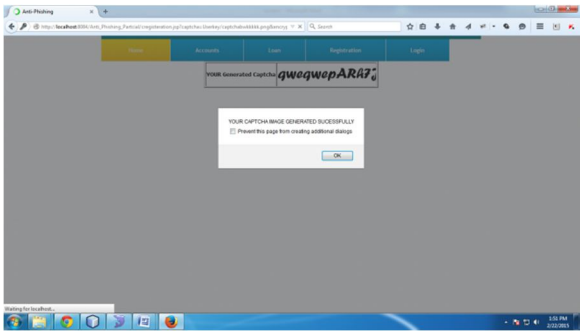

Fig 6.Generation of CAPTCHA

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. 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.

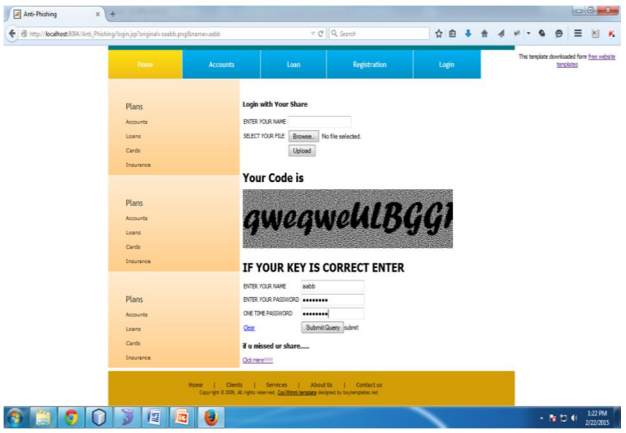

Fig 7.Login Form

VI.CONCLUSION AND FUTURE ENHANCEMENT

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 "Anti-phishing framework based on "Visual Cryptography". The proposed methodology preserves confidential information of users. Verify 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), then in that situation, 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 financial web portal, banking portal, online shopping market. This application can be implemented for all kinds of web application which needs more security.

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords:Learning from the first twelve years," ACM Comput. Surveys, vol. 44,no. 4, 2012.

[2] (2012, Feb.). The Science Behind Passfaces[Online].Available:http://www. realuser.com/published/ .pdf

[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.

[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of Graphical passwords," Int. J. Netw. Security, vol. 7 ,no. 2, pp. 273–292, 2008.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password System ,"Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.

[6] P. C. van Oorschot and J. Thorpe, "On predictive models and user drawn Graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, No. 4, pp. 1–33, 2008.

[7]J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in Proc. ACM CCS, 2008, pp. 543–554.

[8] G. Mori and J. Malik, "Recognizing objects in adversarial clutter,"in Proc. IEEE Comput. Society Conf. Comput. Vis. Pattern Recognit., Jun. 2003, pp. 134–141.

[9] G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs," in Proc. IEEE Comput. Soc.Conf. Comput. Vis. Pattern Recognit., Jul. 2004, pp. 23–28.