ANTI Phishing Framework with Visual Cryptographic and Dynamic Captcha Schemes

Anup Redkar[1] Shailesh Dhanawade[2] Abhishek Bilare[3] Nilima Patil[4]
[1]Engineering Student, [2]Engineering Student, [3]Engineering Student, [4]Assistant Professor
[1]Computer Engineering Department,
[1]K. C. College of Engineering and Management Studies and Research, Mumbai, India

***Abstract**:* Phishing is a routine method of online identity theft and virus spreading using forged web pages. For phishing detection and prevention a new methodology is used to detect the phishing websites based on the Anti-Phishing Image CAPTCHA using visual cryptography with dyanamically generated CAPTCHA schemes. It generated CAPTCHA for every new transaction or any operation done which will affect the system or change the system. Every new CAPTCHA generated the first share will be mailed to the user and the other half at the server. When the user uploads his half to the server if it matches CAPTCHA will be shown. Every time the user will get a new CAPTCHA and the splitting process will be done. Resulting into shares of CAPTCHA.

IndexTerms – **CAPTCHA, Visual Cryptography.**

I. INTRODUCTION

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 identity theft, financial gain and other fraudulent activities. In this paper we have proposed a new approach named as "A Novel Anti-phishing framework based on visual cryptography" to solve the problem of phishing.

Here an image based authentication using Visual Cryptography (VC) is used. The use of visual cryptography is explored 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.

II. PROPOSED SYSTEM

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.

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.

1. (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.
2. (n, n) -Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares is combined will the secret image be revealed.

3. (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.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Figure.1 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.

Advantages of Proposed System:

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.

The proposed system is based on the CAPTCHA. A random number session key (CAPTCHA) is generated by the system and user has to store it for further reference during the login. The CAPTCHA consists of three random characters which are required during the login stage. Proposed system architecture is shown in Figure 3.1.

The proposed system consists of three modules:

- User Registration
- CAPTCHA
- Login

The proposed authentication system works as follows:

User registration phase includes the registering the users to the system. For registering to the system user have to click on the “new user registration” button. It will display a registration form. For registration the users have to first enter his username and the other relevant data that is given in the registration form. The username must be unique to the system. The system will check whether the username is already existing in the database or not. He will also have to set a password which is alphanumeric in nature and should be strong enough. The details of the user obtained from the registration form are stored in the database. After filling the registration form successfully, the user enters to the “CAPTCHA” module.

CAPTCHA will be generated which the user has to enter to valid his authenticity. This CAPTCHA is to be remembered for future reference. Finally click on the “Finish” button to complete the registration phase.

For authentication (Login) the user first enters his unique user id (username) and his alphanumeric password. Then click on the “Next” button. click on “Next” button the CAPTCHA key has to be entered in the box as the final step of authentication. If the CAPTCHA key are correct then user can successfully logon to the system

2.1 System Block Diagram:

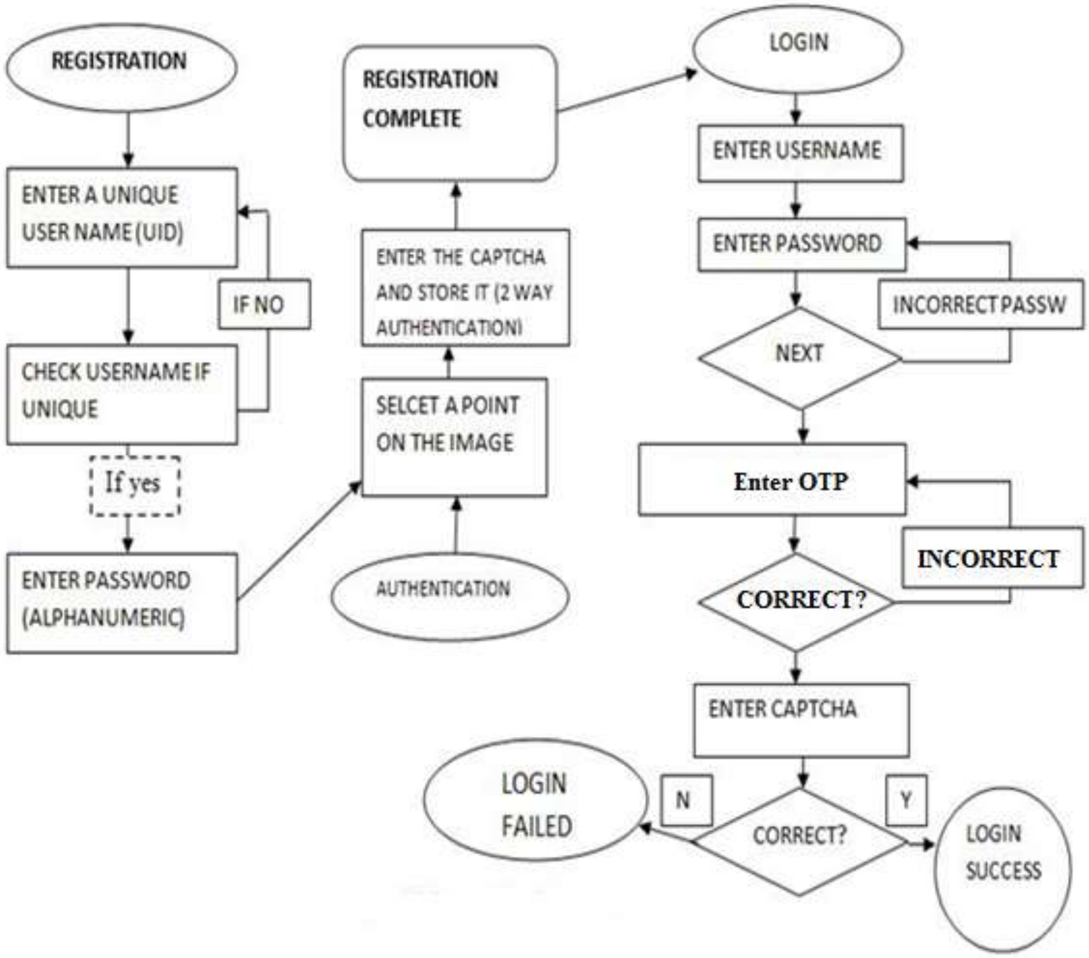

Figure 3.1 System Block Diagram

III. APPLICATIONS

The following are the applications of the project:

4.1. Military :

It is useful for military because whichever the confidencial data they are sending to there user should be safe . It should not be leaked .

4.2. Banking :

It will also be used for secure transaction of money and the useful data such as OTP, bank details of the customer.

IV. ACKNOWLEDGEMENT

We wish to express our deep sense of gratitude to our Project Guide Prof.Nilima Patil for guiding us for the project. We sincerely acknowledge for giving their valuable guidance and critical reviews and comments.
Finally, we would like to express our heartfelt thanks to all supporting staff members and friends who have been a constant source of encouragement for completion of the project.

V. CONCLUSION

Thus we propose to develop a two-way encryption based 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.

Important issues will be resolved such as Security, and authentication will be addressed and resolved.The proposed system has been designed to improve performance and efficiency of existing system. It is the application that has increased the capability of existing system.

VI. REFERENCES

i. A Novel anti-phishing framework on cloud based on Visual cryptography, Nagesh soradge, K. S. Thakare, , Proceedings of 12th IRF International Conference, 29th June-2014, Pune, India, ISBN: 978-93-84209-31-5

ii. Anti-Phishing Framework for Banking Based on Visual Cryptography, K. A. Aravind, Mr. R. Muthu Venkata Krishnan, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January- 2014, ISSN: 2321-8363

iii. An Anti-Phishing Framework using Visual Cryptography, International Journal of Advanced Research in Computer and Communication Engineering , Abhishek Thorat, Mahesh More, Ganesh Thombare, Vikram Takalkar, Manisha N. Galphade, Vol. 4, Issue 2, February 2015

iv. Anti Phishing using Visual Cryptography, International Journal of Science and Research (IJSR) , Amit Navarkar, D. A. Phalke, ISSN (Online): 2319-7064 Volume 3 Issue 2, February 2014.