Prevention of Phishing Attacks with the Help of Anti-Phishing Website using Visual Cryptography (Banking Portal)

Prof. P. V. Waje – Kashid[1] Saheel Deshpande[2] Sadhana Dhokane[3] Chetan Nagare[4] Neha Pawar[5]
[1]Guide [2,3,4,5]Student
[1,2,3,4,5]Department of Information Technology
[1,2,3,4,5]SVIT, Nashik, India

Abstract— For security purposes every application provides user authentication. From a very long time secret data or computer code has been used for giving security to information. In user authentication we have to complete the process of entering username and password. Authentication process has 3 parts Token based, Biometric and Knowledge based authentication. Almost all existing web applications are providing knowledge based authentication including alphanumeric passwords as well as graphical passwords. In today's changing world when we are having number of networks and personal accounts some secure authentication method is required. In the process of phishing an individual, group tries to thieve personal and confidential information of the user such as passwords from unsusceptible victims for the purpose of identity theft, financial gain and other fraudulent activities causing loss. A new approach has been proposed in this paper called "An 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 VC scheme method is explored to preserve the privacy and security of image captcha. It decomposes 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 image captcha. Once the original image captcha is revealed to the user it can be used as the password. In the above mentioned approach we provide image based authentication, where password image is generated for every login attempt and it will be downloaded from the registered email of the user which has been used for registration. Every time the image generated is unique.

Key words: Visual Cryptography Scheme (VC), Phishing, Authentication, Anti-Phishing

I. INTRODUCTION

Nowadays bank transaction e-commerce, online booking system, etc are very common. So various attacks can hazards the information used while performing above mentioned activities. Phishing is one of them in which illegal activities are performs using different social engineering techniques. Attackers try to acquire important information such as password, credit card details and confidential data. Definition of phishing state that Phishing is the fraud method in which sensitive information is acquired by masquerading as a trustworthy for his/her economic or individual gain. Communication channels such as websites, e-mails and instant messaging services are very popular. So in these cases phisher /attacker can easily thieve the information of the authorized user.

For security purposes every application provides user authentication. From ancient days secret data or code is used for hiding and living security to information in user authentication the process which we have to pass through is username and password.

II. LITERATURE SURVEY

In most of the existing system the user login to the online banking system by providing username and password. There is no additional security is provided in the existing system. So if that site is a phishing site then the phisher can capture this information. So the existing system is having lack of security. There are many techniques in order to prevent from phishing attacks but they have several disadvantages.

- Blacklist DNS based anti-phishing method – It maintains a blacklist and detects websites that are not on a blacklist. Since the phishing websites have short life time the accuracy of a blacklist is not too high.
- Heuristic-based anti-phishing approach - It is easy for an attacker to use technical means to avoid the heuristic characteristics detection.
- Similarity assessment based technique – It is time-consuming. This technique has low accuracy and is not perfect.
- An offline phishing detection system - LARX (Large scale Anti phishing by Retrospective data exploration) is not dynamic to real world events.

To avoid such disadvantages and limitations of an existing system there is a system which will able to avoid limitations of the existing system. The proposed system will help websites from phishing attacks. Here we are using visual cryptography technique.

III. EXISTING SYSTEM

Existing system includes the technique such as installation of key logger, screen capture, man in the middle attacks, tricking customers through e-mails and spam messages. To avoid these attacks existing technique like one time passwords, personal identification number, text captcha can be used. But by using these existing techniques we are not able to analyze the phishing sites.

IV. PROPOSED SYSTEM

Main objective of the proposed system is to avoid phishing attacks on websites. In this proposed system a user can identify whether the site is a genuine website or phishing website. This is achieved by verifying the image captcha generated at the time of login. Only a genuine website can reconstruct the image captcha because it holds the other share.

The proposed method also helps to authenticate the user and this is achieved through image based authentication. In this approach we provide image based authentication,

password image is generated for every login attempt and it will be downloaded from the email which has been used for registration. The system checks whether the user is an authorized user or not. Use of image captcha will help to distinguish between users and machine users in that case image captcha is readable by human users. The proposed system is very useful to prevent from phishing attacks.

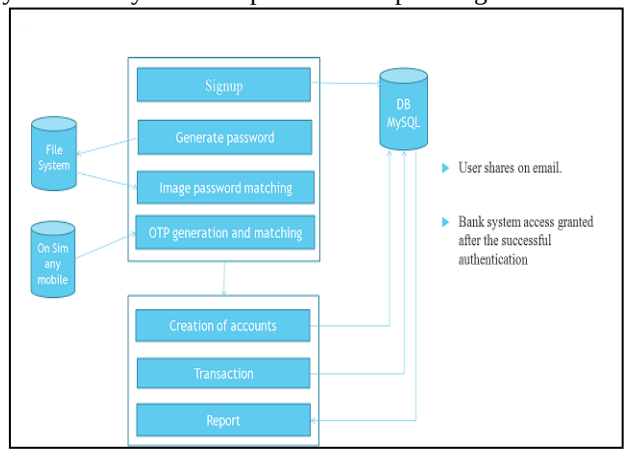

Fig. 1: Proposed System Architecture

V. User Registration Phase

Bank provides the online banking. In this phase user registration is done with the help of VC Algorithm. While registration of user with visual cryptography user is provided by the random images that server have. Among these images user select one image for visual cryptography. The selected image need to remember by the user which is needed in future. After the selection of image Visual Cryptography algorithm is applied on that image. Output of this phase will give two shares. Out of which first share goes under the process of phase two. And second share will recorded to server side with user id and original image. Second the OTP will generate on user mobile. For authentication on the user credential which will also help for strong security.

A. Detection of Phishing Site

When user goes for a transaction, user needs to upload the share one. After uploading, server will request for private key. User need to provide private key assigned during registration (in phase two). Now server is with share one and private key. Then server identifies the user from that key. Now server stacks its share two with users share one by Visual Cryptography. A new image is formed from these two images. Server will check that image with the original one while user also checks formed image with original image selected in phase one. If formed image is same as original image then proceed further transaction and if it is not phishing is detected and user can terminate the transaction without any loss of confidential data.

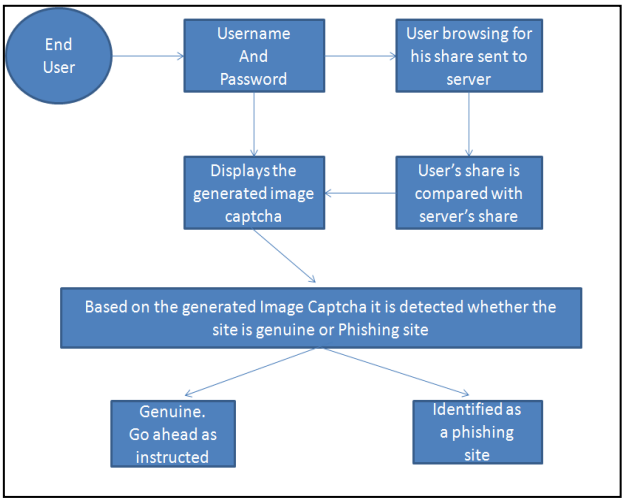

Fig. 2: Detection of Phishing Site

VI. Expected Result

- The user's credentials are safe and secure from phishing attacks.
- Providing security using new technology like virtual cryptography.
- The proposed methodology preserves confidential information of users using image based authentication.

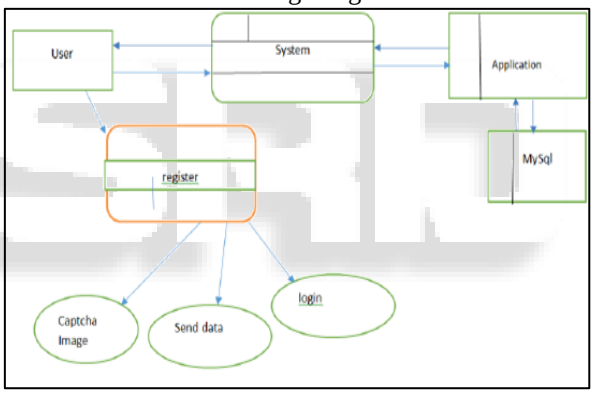

Fig. 3: Data Flow Diagram

VII. Conclusion

From this it is concluded that Phishing websites can be easily identified using our proposed "Anti-phishing websites using Visual Cryptography". The proposed methodology preserves confidential information of users using image based authentication. 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. The proposed system is very useful and will prove to be more secure to prevent phishing attacks.

VIII. Acknowledgment

We express deep sense of gratitude to our project guide Prof. P.V. Waje-Kashid , Head of Department, Prof. R.S. Bhalerao and all the staff members of the Department of Information Technology, for their valuable time, support, comments, suggestions and persuasion. We would like to extend our sincere thanks to our family members. It is our privilege to acknowledge their cooperation during the course of this

project. We express heartiest thanks to our known and unknown well-wishers for their unreserved cooperation, encouragement and suggestions during the course of this project.

REFERENCES

[1] Online fraud transaction prevention system using extended visual cryptography and QR code, Shubhangi Khairnar, Reena Kharat,2016 International Conference on Computing Communication Control and automation (ICCUBEA),Year: 2016,Pages: 1-4

[2] "Madhusudhanan Chandrasekaran Ramkumar Chinchani Shambhu Upadhyaya, PHONEY: Mimicking User Response to Detect Phishing Attacks, WOWMOM '06 Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks, Pages668-672, IEEE Computer Society Washington.

[3] Divya James and Mintu Philip 2012, A Novel Anti Phishing Framework Based On Visual Cryptography International Conference on Power, Signals, Controls and Computation(EPSCICON).

[4] Nilkesh Surana, Prabhjot Singh, Umesh Warade, Neha Sabe 2015, Detection and Prevention of Phishing Attacks in Web International Journal of Scientific Engineering and Technology Re- search, ISSN 2319-8885 Vol.04,Issue.[08], April-2015, Pages:1595- 1598.

[5] Shizra Sultan, Abdul Ghafoor Abbasi; Awais Shibli, Secure protocol for financial transactions using smartphones ,Security and Cryptography (SECRYPT), 2014 11th International Conference, 2016.

[6] Dhanashree Moholkar,"An Efficient Approach for Phishing Website Detection using Visual Cryptography (VC) and Quick Response Code (QRCode)", International Journal of Computer Applications (0975 - 8887) Volume 1 15 - No. 12, April 2015.

[7] Gaurav Palande, Shekhar Jadhav," An Enhanced Anti-Phishing Framework Based on Visual Cryptography", International Journal of Emerging Research in Management Technology ISSN: 2278- 9359 (Volume-3,Issue-3)

