A Novel Secure Framework Based On Visual Cryptography

Shubham N. Khalane[1], Laher S. Panchamiya[2], Hrishabkumar R. Jha[3], Sweety Rupani[4]
[1, 2, 3, 4]Department of ECE
[1, 2, 3, 4] Vidyavardhini's College Of Engineering And Technology

Abstract- *Threats on security of website are not addressed thoroughly, so people can't trust online transactions that involve due authentication through credentials. With the arrival of internet, the number of online attacks has increased and the most common attack is phishing. Phishing attack is real threat to security of system. Phishing is a technique used by cyber criminals to get our confidential credentials which we enter in websites. Fake websites which are identical to real websites are used for phishing. To protect user visual cryptography comes to rescue, in our framework we partition a given image into two parts such that one part is with user and other part is with server; the individual images are encrypted but when they are stacked together generates original image or Captcha. Captcha image generated can be used as password to login the system. Also to make system more secure we use concept of OTP with visual cryptography.*

Keywords- captcha, Visual cryptography, security, phishing

I. INTRODUCTION

Phishing is a process of deceiving a party in order to obtain credentials and gain monetary and other gains. Phishing attacks are often not correctly addressed, thus websites in today's world are vulnerable to phishing attack. Phishing attacks mainly occur in banking and e-commerce domains. In attacks on banking sites the cyber criminals steal our important credentials and may get our credit/debit card information and thus can steal money from our respective credit card and bank account. In ecommerce website also in similar way cyber criminals access our important credentials and make spam call or emails to us .In similar way all the sites that need user credentials are vulnerable to attack from cyber criminals by attacks as phishing attack. Thus to stop this criminal activities we have proposed a novel secure framework based on visual cryptography. The proposed framework has two phases. First phase is registration phase where new user registers himself. In this process the user provides his important credentials like name, date of birth, phone number, address. In this registration process user is provided a half part of captcha image. Another half of captcha image is stored at server. Second phase is login phase and it is used for sharing images between client and server. In login phase first the user enters username and password then the user is asked to provide the half part of image, after that system processes information and then proceeds with login phase and if user is successfully verified he is allowed to login the system. To provide extra level of security we are use One Time Password to secure the transaction and Google Re-Captcha is also used by us to detect bots attacking our website.

II. AIM AND OBJECTIVE

This framework is used to protect user from any kind of phishing attack and to secure the credentials of user. Also it is integrated with One Time Password to make it more secure and effective.

III. SCOPE

This framework can be used on any websites or applications where user are required to enter confidential information in website or in application. For example banking websites, Online shopping websites etc.

IV. LITERATURE SURVEY

Phishing attack is performed by attacker by a series of actions. This is done by use of spam mails or by use of a phishing website. One of the best technique to protect user is by use of Cryptography. In this technique data is encrypted and user and server can only decrypt the data. Naor and Shamir [1] has given the concept of visual cryptography in which images are shared secretly to securely login user to system.

Visual cryptography techniques are also proposed by Shamir and Blakley [2], there motive was to prevent cryptographic technique from getting affected by any error also here visual cryptography is used.
A segment-based visual cryptography introduced by Borchert [3] technique was to encrypt information containing numbers, as bank account number, bank balance amount, etc. The VCS proposed by Wei Yan et al. [4], technique can be applied to only images and printed text, in which cryptography shares of images are generated.

In 2000, Ren-Junn Hwang [3] has given a watermark method that is very popular method to protect copyright of digital image.

V. VISUAL CRYPTOGRAPHY

Visual Cryptography Scheme is a technique of cryptography where encryption of a visual data is performed using encryption methods and decryption is possible by use of human visual system that is eye.

This can be achieved by one of following techniques or schemes:

1] (2, 2) Threshold Visual Cryptography scheme-

In this scheme secret data is in form of images from this secret data 2 shares of images are produced, the original data can be only retrieved if these two shares are stacked together. No additional data is required to access image.

2] (2, n) Threshold Visual Cryptography scheme-

In this scheme the secret data image is encrypted into n shares that is n share of image are generated, to reveal the original image two or more shares of images must be stacked together.

3] (n, n) Threshold Visual Cryptography scheme-

In this scheme the secret data image is encrypted into n shares that is n share of image are generated. To reveal the original secret image all n shares of images must be stacked together.

4] (k, n) Threshold Visual Cryptography scheme-

In this scheme the secret data image is encrypted into n shares that is n share of image are generated. To reveal the original secret image at least k shares of image must be stacked together

In the case of (2, 2) Visual Cryptography Scheme, all pixel named X of original secret image are encrypted into 2 sub pixel called shares. Fig 1 denotes the shares or parts of a white pixel, this pixel acts as original image pixel and a black pixel, this pixel acts as original image pixel. Now the shares of original image pixel that is white pixel and black pixel is randomly determined (there are two possible situations for each pixel). None of shares let us to recognize original image pixel that is white or black pixel. Since all pixels in the original secret image will be encrypted to generate shares by random independent selections. If the two shares of original image pixel are stacked or combined, then the value of the original pixel X that is white or black pixel can be determined. If X that is pixel of original image is black pixel then 2 blacks shares or sub pixel are generated and if X is white pixel the one black subpixel and one black subpixel is generated Our share generation scheme used for our framework is as in figure 2

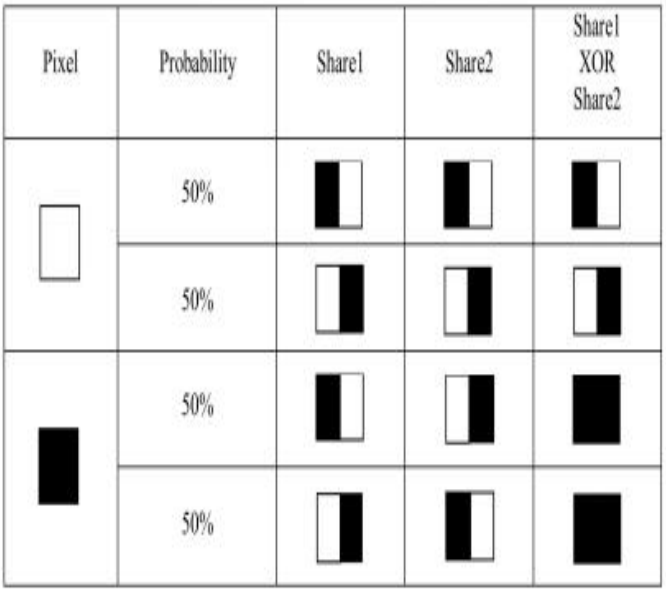

Figure 1: Scheme of encoding binary pixel into two shares

Share Generation Algorithm

Steps:

- Read Image (QR image)
- Get height and width of that image.
- Apply cryptography :

1] Create share 1 by generating random (2*2) matrix

2] Fill this matrix (0, 1) using random value.

- Share 1 XOR with pixel of original image.
- Share 2 is created.

Figure 2: Share Generation Algorithm Used In Our Framework.

VI. EXISTING SYSTEM

In current scenario user enter confidential information in websites and login or register the website. In such case the attacker may generate a phishing website and can obtain confidential information from user as shown in above figure 3

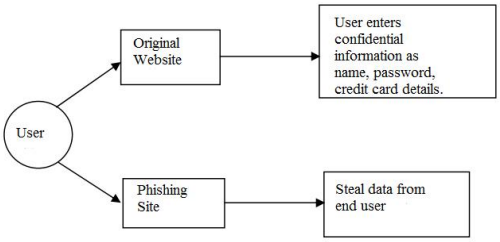

Figure 3: Current Methodology.

VII. WORKING OF SYSTEM

In registration phase, as shown in figure 4, the user enters a password and username and server also enters a password. Now with the help of this keys or password user is given or displayed a captcha image by the server. Half part of image is stored at server and half part of image is stored at client or user. In this way we generate two halves of images which are compared at login phase as user enters one half and server enters other half to login system. After user successfully logins the system he can also be verified again for two step verification with one time password. Also to detect bots visiting the website and to stop the entry of bots in website we can use Google Re-Captcha.

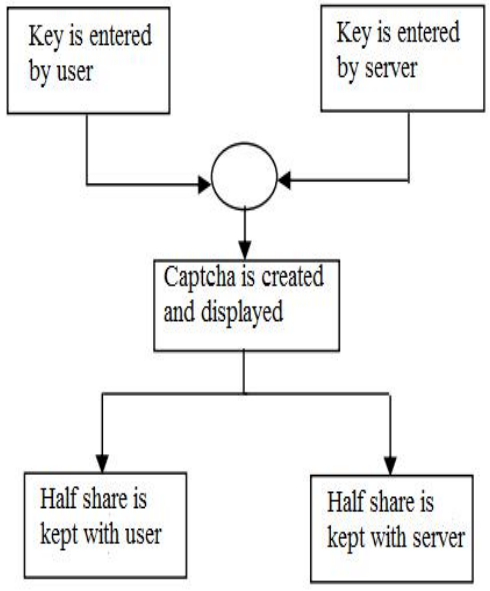

Figure 4: Registration process in short.

VIII. PROPOSED METHODOLOGY

This system works in two phase as
1. Registration Phase
2. Login Phase

1. Registration Phase

In Registration Phase as shown in figure 5, user is allowed to enter his personal credentials as name mobile number, address, password and credit card details. After successful entry of details user can be verified by Google Re-Captcha or by any other bot detection method. Then captcha image is divided in two parts at server end, one part of it is given to user and other part is kept at server. After successful completion of registration phase user proceeds with login phase

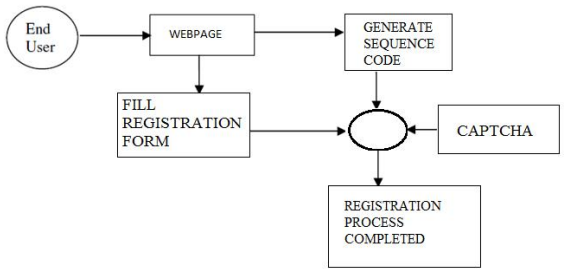

Figure 5: Registration Phase

2. Login Phase

In login phase as shown in figure 6, user enter his username and password then user is requested to enter his half share of image. Once user enter half share of image it is stacked with other half which is stored with server, this generated image is verified for its authenticity, once image is verified user is asked to enter captcha on image then again for double step verification verified with One Time Password. Bots can also be detected using Google Re-Captcha. After this user is allowed to login the system.

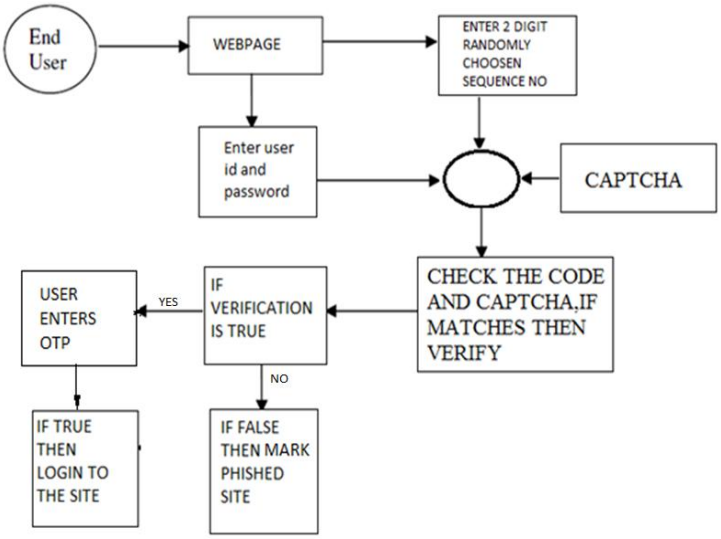

Figure 6: Login Phase.

IX. CONCEPT OF SHARES

In this we consider Fig 7 that is case 1, where the original image is encrypted into two shares and decryption is only possible if the two shares are stacked together as shown in Fig 7

Also in Fig 8 that is case 2, same process is mentioned But in Fig 9 that is case 3, if Share of one image is merged with share of other image then an image is generated that is not recognizable or an inconsistent image is generated.

CASE.1

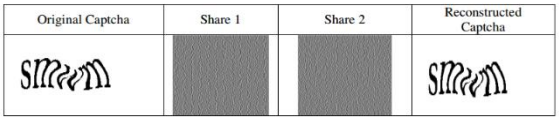

Figure 7 Case 1

CASE.2

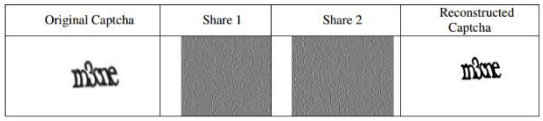

Figure 8 Case 2

CASE.3

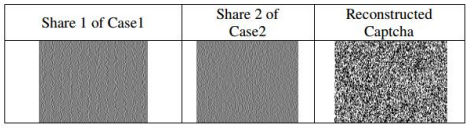

Figure 9 Case 3

X. DATA FLOW DIAGRAMS

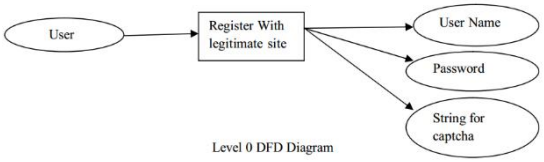

Figure 10: Level 0 DFD Diagram

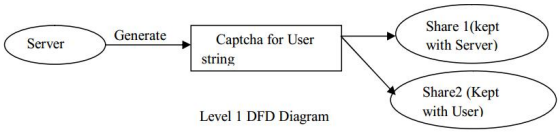

Figure 11: Level 1 DFD Diagram

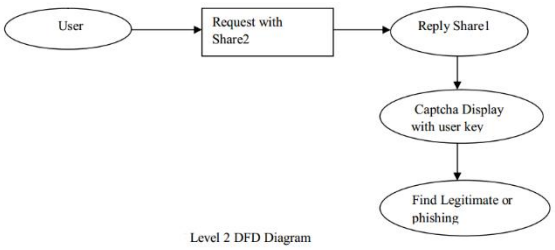

Figure 12: Level 2 DFD Diagram

XI. HARDWARE AND SOFTWARE REQUIREMENTS

Hardware Requirements:

System : Pentium IV 2.4 GHz or higher.
Hard Disk : 40 GB or greater.
Monitor : 15 VGA Color.
Ram : 512 Mb or greater.

Software Requirements:

Operating system : - Windows XP.
Coding Language : ASP.NET, C#.Net.
Data Base : SQL Server 2008

XII. EXPERIMENTAL RESULTS

In registration phase as shown in fig.13 first of all we have to enter the important credentials of user as name, phone number, date of birth, address. Then user enters text on captcha image and registers. In this way we successfully register the user by entering above details, after that user is provided half part of captcha image that is used to secure the login process and registration process.

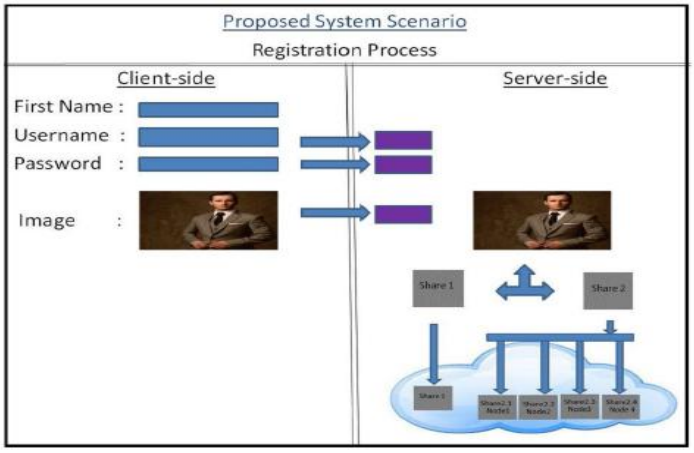

Figure 13: Real Time Working (Registration).

Now during the login process as shown in fig.14 the user enters the username and password which is taken as input

and compared with data in database at server end. After that user has to provide half part of image that is stored at user end. Once user uploads the image on his side then server stacks the half image given by user with the half image stored at server end and generate an image .If the generated image is accepted as correct image then user is asked to enter text on captcha and then user is allowed to proceed the login process and is allowed to login, else if image is false image then user is blacklisted and not allowed to login with that particular username. This process can be made more secure by use of free methods of visual cryptography as Google Re-Captcha and by the use of One Time Password. In Google Re-Captcha we are asked to choose right image from given set of images and if we choose wrong image then again a different set of images are provided and this continues until we enter right set of images. For example: If Google Re-Captcha asks to provide images of cars from given set of images then we have to select cars images and only then we can proceed. One Time Password can be also used for double step verification which can be provided on mobile or email-id of user.

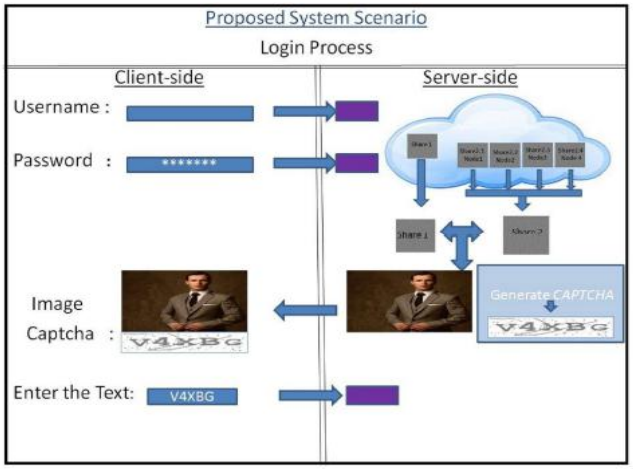

Figure 14: Real Time Working (Login).

XIII. CONCLUSION

Phishing attack is commonly performed in today's generation, but it is not correctly addressed. Even though phishing attack is wide spread no exact solutions are there to stop this attack That's where our secure framework comes to rescue. In this framework we provide two layer security .Firstly we let user and server identify whether the website is phishing website or not. This is achieved as the phishing website cannot generate the actual captcha image as half image at server end is not stored at server end of phishing website and thus phishing website cannot generate captcha image.

Secondly the user is asked to enter text on captcha image during login phase. Now this step of system protects user and website for entry of bots in the website. Thus captcha protects website from entry of bots.

Thus by using visual cryptography by use of captcha, we protect user from phishing attacks that are difficult to prevent and also we protect website from bots.

XIV. FUTURE SCOPE

Using visual cryptography we have created a system that is a one-step verification system. But it can be integrated with other techniques for example as watermark technique to make this system or framework more effective and resistant to any attacks.

Also this system can be used for banking websites to secure the banking transactions, also in healthcare websites to secure credentials of patients and in e-commerce website to secure the e-commerce transactions

ACKNOWLEDGEMENT

We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend my sincere thanks to all of them.

We are highly indebted to Prof. Sweety Rupani for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

We would like to express my gratitude towards my parents & member of Vidyavardhini's College Of Engineering And Technology for their kind co-operation and encouragement which help me in completion of this project.

Our thanks and appreciations also go to my colleague in developing the project and people who have willingly helped me out with their abilities.

REFERENCES

[1] A. Shamir and M. Naor, Advances in Cryptology EUROCRYPT, "Visual Cryptography".

[2] G. Blakley, Proceedings of AFIPS Conference , "Safeguarding Cryptographic Keys".

[3] Borchert, WSI Press, Germany,"Segment Based Visual Cryptography",, 2007.

[4] M. S. Kanakanahalli, and D. Jin, W-Q Yan, "Visual Cryptography for Print Applications", IEEE.

[5] Ren Hwang, *Tamkang* Journal of Science and Engineering," A digital image protection scheme based on visual cryptography",

[6] A Novel Anti Phishing Framework Based On Visual Cryptography Shital B. Patil, Uma Nagaraj. Student, M.I.T., Pune, Maharashtra.

[7] A Novel Antiphishing framework on Cloud Based On Visual Cryptograpghy Nagesh Soradge , K. S. Thakare Sinhgad College of Engineering , Vadgaon. Pune, India.

[8] Anti-Phishing framework based on Extended Visual Cryptography and QR code Shubhangi Khairnar ME Scholar Pimpri Chinchwad College of Engineering.

[9] A Novel Anti Phishing Framework Based On Visual Cryptography Mounika Reddy.M1, Madhura Vani.B Student, Department of CSE, MLRIT, Hyderabad, India.

[10] Novel Authentication System Using Visual Cryptography Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana Symantec Software India Pvt. Ltd., India.