Secure Server Verification

Shweta Umredkar[1], Snehal Badhe[2], Hemali kondhekar[3]

Abstract— The fame of Internet and its merits are being highly masked by the drawback associated with it. Out of them the prime issue is internet vulnerability which ultimately leads to data modification and information thefts. Many Web applications store the data in the data base, retrieve it and update information as needed. The approach is divided into two phases that is registration phase and login phase. In the registration phase, the key string is asked from the user, which in turn is concatenated with randomly generated string in the server and an image captcha is generated. It is based on Anti-Phishing Image Captcha validation scheme using visual cryptography. Blacklist database technique cannot detect the websites that are not in the blacklist database[8]. Heuristic based anti-phishing technique is easy for hackers to use technical means to avoid the heuristic characteristics detection[8]. Assessment based technique is time consuming[8]. In this paper we have proposed a new approach named as "Secure Server Verification" by using RSA algorithm and Visual Cryptography. Cryptography is the commonly used technique to protect the data. In this paper, image is not generated, rather it is provided by the server or user can browse the image as well. Attackers would not be able to crack the encrypted image by any technical means.

Index Terms— Encryption algorithm, Decryption algorithm Phishing, Security, Visual cryptography

I. INTRODUCTION

Phishes can fake the URL that appears in the address field at the top of user's browser window and redirect him to another web site with the intention of performing fraud. Fraudsters send e-mails with a link to a spoofed website asking you to update or confirm account related information. To avoid such type of attack this application is very important. In this application we use the image authentication. This is done by using the Encryption Algorithm and visual Cryptography. In this system website cross verifies its own identity and proves that it is a genuine website before the end users provide any confidential information.

To solve the problem of phishing, an approach named as "Secure Server Verification" by using RSA Algorithm is used where an image based authentication is done by Visual Cryptography.

The increase in online services offered to consumers has naturally led to an increase in the exchange of personal information to access E-commerce and online banking services. Various online attacks has been increased, one of them is phishing attack. Fake websites which appear very similar to the original ones are being hosted to achieve this. So we have proposed a new approach named as "Secure Server Verification by Using Visual Cryptography" to solve the problem of phishing.

The main purpose of the paper is to safeguard users from fraudulence and identify theft of the users of the system.
The system will be likely to keeps confidential information of the users like, passwords, credit card information etc. from unsuspecting victims for various fraudulent activities.
Every user request will be redirected from web server to secure server and their credentials are matched with the server credentials and upon verification of the credentials the user verifies the server and the transaction is started.

II. LITERATURE SURVEY

Divya James Mintu Philip[1] introduced that the website cross verifies its own identity and proves that it is a genuine website before the end users and make the both the sides of the system secure as well as an authenticated. 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 into shares, such that stacking of shares will reveal the secret image [1].The existing method of VCS uses dithering technique to generate half toned images. In Visual Cryptography Scheme (VCS) there are five phases [1] i.e. halftoning, share Generation, Embedding secret, Extracting secret, reveal secret.

Shweta Umredkar[1], *Computer Department, Savitribai Phule Pune University, Pune, India*
Snehal Badhe[2] *Computer Department, Savitribai Phule Pune University, Pune, India*
Hemali kondhekar[3], *Computer Department, Savitribai Phule Pune University, Pune, India*

ISSN: 2278 – 1323

J. Tamilarasi, V. Vanitha, T. Renuka introduces halftoning is used to convert the grayscale image to binary image. Shares are generated from binary image depending on scheme chosen .First method is General Access Structure (n, n) for which n shares are required to reconstruct the secret. The second method is Threshold Access Structure (k, n) where k number of shares will recover the secret from available n shares where k is less than or equal to n[4]. Cover images are halftoned to generate covering shares. Secret image is embedded into cover image [4]. Reconstructed shares are generated from the embedded shares [4]. This system is proposed for detection and prevention against phishing attack. This approach is based on visual cryptography. It prevents confidential information from the phishing websites [4].

To deal with the security problems, various secret sharing schemes have been developed. One such secret scheme is extended visual cryptography. It is the way for combining visual cryptography and stenography. This extended visual cryptography (EVC) can be applied for the images as well as the text in the image format [4]. The main application of this scheme is to keep the biometric images safe and secret.

III. Limitations Of Previous System

Blacklist database technique cannot detect the websites that are not in the blacklist database [8].

Heuristic based anti-phishing technique is easy for hackers to use technical means to avoid the heuristic characteristics detection [8].
Assessment based technique is time consuming [8].

IV. Problem Statement

To solve the problem of phishing, an approach named as "Secure Server Verification" by using RSA Algorithm where an image based authentication is done by Visual Cryptography.

V. Proposed System

This approach attempts to provide solution to password login attacks, detection and prevention against phishing attacks. It prevents confidential information from phishing sites through two phases:
1. Registration Phase
2. Login Phase

5.1 Registration Phase

In the registration phase, user will provide the profile Information and sends registration request to server Information related to the user profile is stored in the database.

This phase is depicted in fig1.

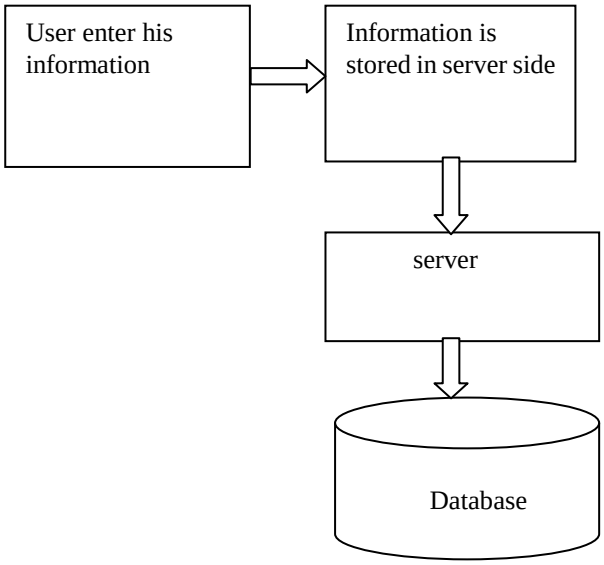

Figure1-Registration phase

5.2 Login Phase

When the user logs in by entering his confidential data for using his account, then first the user is prompted to enter his username and password. Users account is verified, providing the user with the notification popup whether he has successfully login or not.

If login is successful then the user is asked for the selection of image. After image selection, visual cryptography technique of (2, 2) VSC is applied. One share is sent to the user where the another share is kept with the server.

This phase is depicted in Fig.2

ISSN: 2278 – 1323

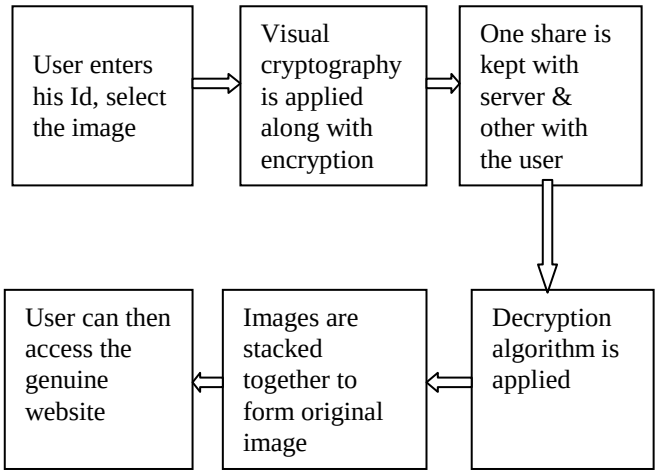

Figure2-.Login phase

5.3 Visual cryptography

Cryptography is the commonly used technique to protect the data. In this technique messages are encrypted and that can be decrypted by only the intended sender or the intended receiver. Various mathematical algorithms are used for encryption and decryption in such a way that no one but the intended recipient can decrypt and read the message.

Visual cryptography scheme (VCS) is introduced by Naor and Shamir. It is a simple and secure way to allow the secret sharing of images. An image is composition of pixels. Each pixel is stored in bits. Thus, the image shown on the stacking of shares is considered as the real secret image.

Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted. When the two shares are stacked together, the value of the original pixel P can be determined.

5.4 Encryption algorithm

1. Get color pixel from image of (x,y) position.
   Color Pixel (x, y) ==> color

2. Separate (A,R,G,B) values from color
   A= (color >> 24) & 0xff;
   R= (color >> 16) & 0xff;
   G= (color >> 8) & 0xff;
   B= (color >> 0) & 0xff;

3. Convert ARGB values to CMYK values.
   R'= R / 255
   G'= G / 255
   B'= B / 255

   K = 1-max (R', G', B')
   C = (1-R'-K) / (1-K)
   M = (1-G'-K) / (1-K)
   Y = (1-B'-K) / (1-K)

   K = K * 255f
   C = C * 255f
   M = M * 255f
   Y = Y * 255f

   K = K/ 5f
   C = C/ 5f
   M = M/ 5f
   Y = Y/ 5f

4. Create two splits by CMYK values
   Slpit1 ==> A
   Slpit2 ==> B

   A ==> put
   Pixel (x, y) ==> (A, R, G, B) ==> (A, C, M, 0)

   B ==> put
   Pixel (x, y) ==> (A, R, G, B) ==> (A, Y, K, 0)

5.5 Decryption algorithm

Split1 ==> A
Split2 ==> B

1. Get color pixel from image of (x,y) position
   int pixA = A.getRGB (i,j);
   int pixB = B.getRGB (i,j);

2. Separate (C, M, Y, K) values from color of A and B Image
   c = (pixA >> 16) & 0xff;
   m = (pixA >> 8) & 0xff;
   y = (pixB >> 16) & 0xff;
   k = (pixB >> 8) & 0xff;

3. Convert CMYK values to ARGB values
   c = 5 * c;
   m = 5 * m;
   y = 5 * y;
   k = 5 * k;

k = k / 255f;
c = c / 255f;
m = m / 255f;
y = y / 255f;
k = k / 255f;

R = 255 * (1-c) * (1-k);
G = 255 * (1-m) * (1-k);

ISSN: 2278 – 1323

B = 255 * (1-y) * (1-k);

4. Create original image from RGB values
   Original image == put
   Pixel(x,y) ==> (A,R,G,B) ==> (A,R,G,B)

VII. RESULT

This paper makes sure that the user accessing a particular websites in order to process the transaction is phished or not. It is expected that this paper does not use time consuming techniques. Also, it won't be easy for the hackers to crack the encrypted image through any technical means over a network.

VIII. CONCLUSION

Phishing is a continual threat that keeps growing to this day. Communications purporting to be from popular social websites, bank sites, auction sites, online payment processors are commonly used to lure unsuspecting public. All these messages or a site tries to trick the users into revealing personal information by appearing to be from a legimate source. Phishing websites as well as human users can be easily identified using "Secure Server Verification". This is done by using the Encryption, Decryption Algorithm and Visual Cryptography.

IX. REFERENCES

[1] Divya James, Mintu Philip, " A Novel Anti Phishing Framework based on Visual Cryptography " , Mtech in Information System Security Department of *Computer Science and Engineering Kochi*, India, Indira Gandhi National Open University Rajagiri *School* of Engineering and Technology Kochi, 2012

[2]Gaurav Palande, Shekhar Jadhav, Ashutosh Malwade, Vishal Divekar, Prof. S. Baj, "An Enhanced Anti-Phishing Framework Based on Visual Cryptography", *International Journal of Emerging Research in Management & Technology* ISSN: 2278-9359(Volume-3, Issue3)

[3] G. Pavithra, D. S.John Deva Prasann," Countering Phishing Threats using Visual Cryptography "*International Journal of Science and Research* (*IJSR),* India Online ISSN: 2319-7064, Volume 2 Issue3, March 2013

[4] J. Tamilarasi, V. Vanitha, T. Renuka," Improving Image Quality in Extended Visual Cryptography for Halftone Images with No Pixel Expansion", *International journal of scientific & technology Research* volume 3, issue 4, April 2014

[5] Shabbir Hussain1, Mufazzal Hussain2, Ganesh Thakur, " Secure Server Verification using Visual Cryptography and RSA Algorithm*", International Journal of Enhanced Research in Management and Computer Applications*, ISSN: 2319-7471 Volume 3 Issue 3, March-2014, pp: (42-47)

[6] H.J. Kim, V. Sachnev, S. J. Choi and S. Xiang,"An Innocuous Visual Cryptography Scheme", in *Proceedings of IEEE-8th International Workshop On Image Analysis for Multimedia Interactive Services*, 2007.

[7] Shital B. Pawar, Prof. N. M. Shahane," Visual Secret Sharing Using Cryptography" *International Journal of Engineering Research* (ISSN: 23196890) (Online), 23475013(print) Volume No.3, Issue No.1, Jan. 2014

[8] Mangala S. Wale, Gayatri M. Bhandari," Anti Phishing Approach Using Probabilistic (t, ∞) VC Scheme" *International Journal of Advanced Research in Computer Science and Software Engineering.*ISSN:2277 128X, Volume 3, Issue 10, October 2013

ISSN: 2278 – 1323