IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Anti-Phishing I-Voting System using Visual Cryptography

Ramya. R. Nelli[1], Rashi Mehra[2], Pallavi Madri[3], Monica S[4], Rajeshwari J[5]

Student, Information Science Engineering, Dayananda Sagar College of Engineering, Bangalore, India[1,2,3,4]

Associate Professor, Information Science Engineering, Dayananda Sagar College of Engineering, Bangalore, India[5]

Abstract: Anti-phishing I-voting system using Visual Cryptography (VC) aims at providing a facility to cast vote for critical and confidential internal corporate decisions. The user or the employee is allowed to cast his or her vote from any remote place. The election is held in full confidentiality where the user is allowed to vote only if he logs into the system by entering the correct password. The password is generated by merging two shares using VC scheme. Before the election administrator sends share 1 to the voter's e-mail id and share 2 will be available in the voting system for his login during election. Voter then combines share 1 and share 2 using VC to get the secret password. No information can be revealed by observing any one share. Phishing is an attempt by an individual or a group to get personal confidential information from unsuspecting victims. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter personal information at a fake website.

Keywords: Authentication, visual cryptography, image captcha, phishing, online voting.

I. INTRODUCTION

Network security is involved in many organizations, enterprises and other types of institutions. It involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose ID and password or other authenticating information provided by the network administrator that allows them to access the information and programs within their authority.

Internet is the large and global network. There are different kinds of applications based on the Internet. One of them is online voting system. The use of new technologies to support voting is the subject of great debate. Several people advocate the benefits it can bring such as improved speed and accuracy in counting, accessibility, voting from home and it is also concerned with the risk it poses, such as unequal access, violation to secrecy, anonymity and alteration of the results of an election.

Phishing attack is identified as a major attack among all online attacks. Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Attacker creates a replica of original website or attacker sends a lot of email to the user asking him to change certain confidential data as shown in Fig 1. User then fills and submits the sensitive and useful information into the fake website which allows the attacker to pull the information and save the data for his or her own illegal use.

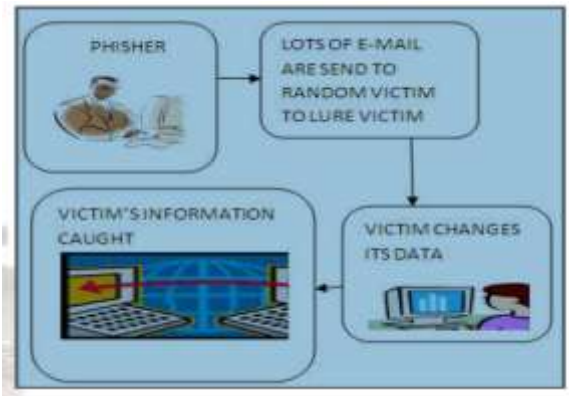

Fig 1: Phishing Attack

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

So, by using visual cryptography technique the problems of online voting system such as security risk and phishing attacks can be prevented. It provides secured authentication for Internet voting system.

II. SECURITY ATTACKS

Confidential data can be vulnerable to any one of following attacks:

1. Eavesdropping
It is secretly listening to the private conversation without their consent. In general, majority of network communications in an unsecured format, allows an attacker to listen or interpret the traffic. It is also known as sniffing or snooping.

2. Data Modification.
After an attacker has read your data, the next step is to alter or modify the original data. An attacker can modify the data in the packet without the knowledge of the sender or the receiver.

3. Identity spoofing.
It refers to the action of assuming the identity of some other entity and then using that identity to accomplish the goal. Most network and operating system use IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be false assumed which is known as IP address spoofing.

4. Denial of Service attack
It is a cyber attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disruption services of a host connected to the internet.

5. Man in the middle attack
A complex form of IP spoofing is the man-in-the-middle attack, where the hacker monitors the traffic that comes across the network and introduces himself as a stealth intermediary between the sender and the receiver.

6. Phishing attack
Phishing is an attempt to criminally obtain sensitive information such as usernames, passwords, by masquerading as a trustworthy entity. It is typically carried out by email or instant message. The phisher often directs the users to enter their confidential information at his fake website.

III. EXISTING SYSTEM

I. Paper ballot system
II. Electronic voting system
III. Online voting system: Online voting system is the latest electronic voting system introduced in which the voted ballot is transmitted over the public Internet through web browser. The voter can directly vote online from anywhere in the world.

IV. DISADVANTAGES OF EXISTING SYSTEMS

(i) Most of the applications are giving high protection towards the Password Security and they are not concentrating on phishing attacks. By phishing, attackers are directly getting the passwords from the user and they can enter into the relevant web sites with correct password.

(ii) There is no efficient technique to safe guard the users of phishing websites.

(iii) Existing system is time consuming and voters has to be in voting booth in presence and it is not feasible when the voters are in other city or in other country.

V. VISUAL CRYPTOGRAPHY

Phishing attacks are prevented by visual cryptography. Visual cryptography is a key-less encryption technique where the decryption can only be done by human eyes. Naor and Shamir introduced the Visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images and data without any cryptographic computations as shown in Fig 2.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Fig.2 Visual Cryptography

Visual cryptography is very useful and safe for I-voting system. The system is web based application so that it can be accessed by any authorized person anywhere in the world through internet. Firstly, the textual password image is converted into black and white images based on RGB (red, green, blue) values.

$$R + G + B / 3 \qquad \text{----- 1}$$

For Each pixel in the monochrome image, the pixel will be divided into 4 sub pixels depending on the colour of the pixel and thus, increasing the size of whole image. There are 6 possible permutations to divide a pixel into 4 sub pixels (2 black and 2 white) as shown in the Fig 3.

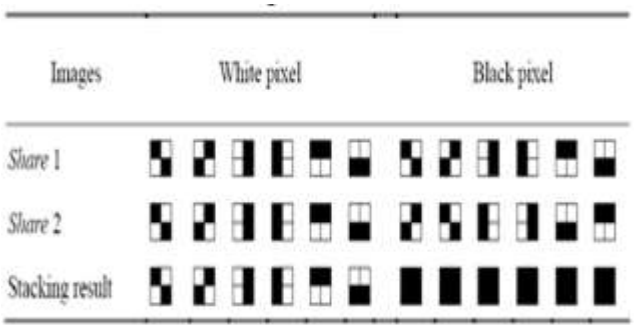

Fig 3: Possible combinations of sub pixels

If the colour of the pixel is white, then one of the possible sub-pixels is as shown in the Fig 4.

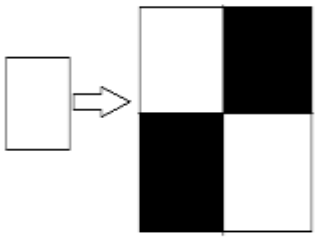

Fig 4: White Sub Pixel

If the colour of the pixel is black, the sub pixel is as shown in the Fig 5.

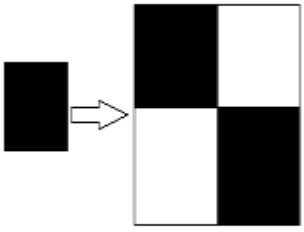

Fig 5: Black Sub Pixel

White pixel is called as an empty pixel and black pixel is called as the information pixel. If the source pixel in the monochrome image is black, then the sub pixels in share 1 and share2 will be inverted as shown in the Fig 6.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

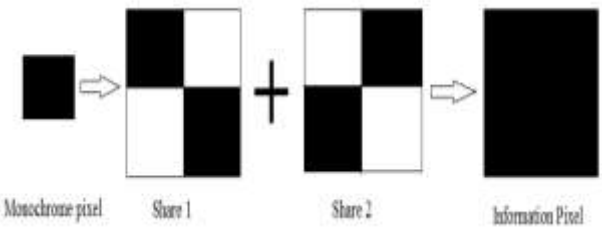

Fig 6: Merging Process for Black Pixel

If the source pixel in the monochrome image is white, then the sub pixels in the share1 and share 2 will be identical as shown in the Fig 7.

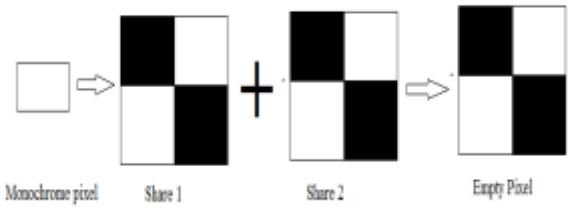

Fig 7: Merging Process for White Pixel

The result of the overall process after merging the two shares is an image containing the textual password which will be represented by information pixels (black pixels) as shown in the Fig 8.

Fig 8: Password Generation

VI. PROPOSED METHODOLGY

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. The proposed methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It will allow only authenticated users to cast vote. Also it will prevent phishing attacks in the internet voting system. The system architecture is shown in Fig 9.

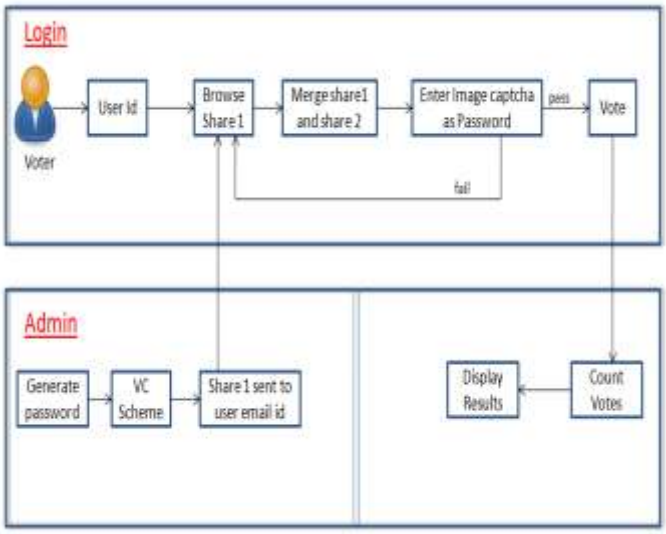

Fig 9: System Architecture

DOI10.17148/IJARCCE.2017.6522

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

The proposed approach can be divided into two phases:

Registration Phase

In the registration phase, the server will pick textual images as passwords. The text of these images will act as the password for the user. The image 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 is sent to the user for later verification during login phase. The image is also stored in the actual database of website as confidential data. Registration process is depicted in Fig 10.

Login Phase

In the Login phase first the user is prompted for the 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. 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. Now, the user id and password will be sent to authentication system for the purpose of authentication. Authentication is the process of ensuring that the person is the one who he claims to be. For this purpose user id is sent to server and corresponding password is fetched from the database. Now the password provided by the user and the password fetched from database is compared. Therefore, 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 and can also verify whether the user is a authenticated or not. Fig 11 can be used to illustrate the login phase.

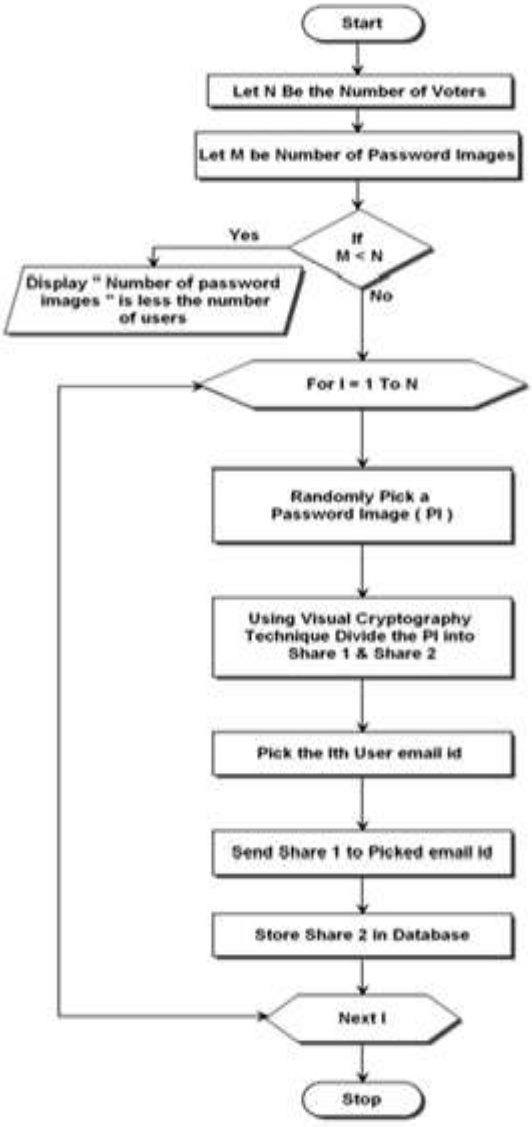

Fig 10: Registration Phase

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

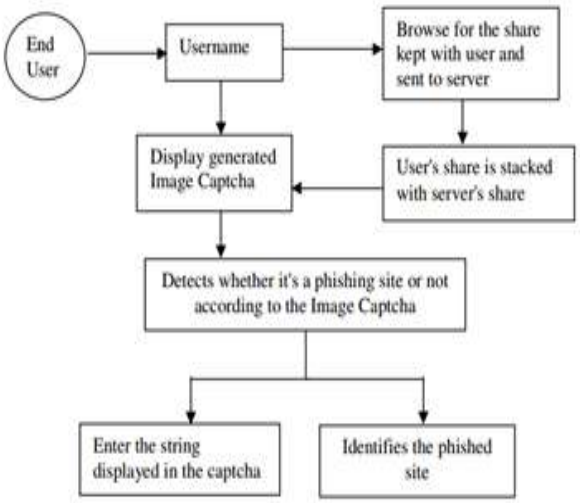

Fig 11: User Login Phase

VII. RESULTS

A. As shown in Fig 12. If the password text is visible to the user after merging share 1 and share 2 then it indicates that the user is authenticated and has entered the genuine website.

Fig 12: Valid password

B. As shown in Fig 13. If the password is not visible (blur image) then it indicates that the user has not provided the correct share. If 2 invalid shares are merged then we do not get the password. This indicates that the website is not genuine and the user is not authenticated.

Fig 13: Invalid password

C. As shown in Fig 14. If unregistered user tries to login then an error message stating invalid user id will be displayed.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Fig 14: Invalid user id

D. As shown in Fig 15. If a user tries to vote more than once for a particular category then an error message stating candidate already voted will be displayed.

Fig 15: Invalid user id

VIII. CONCLUSION

Day by Day population is increasing enormously which in turn demands improvement in the current voting system. Security plays a major role in I-voting. The proposed method uses Visual cryptography to prevent the rapidly growing phishing attack. If this method is implemented, it will be useful for the voters and organization in efficiently reducing cost and time. The physically disabled and aged people can gain a significant advantage of this I-voting system and can cast their valuable votes in a secured manner for all the critical decisions of corporate companies. The proposed methodology allows a user to vote only once. It verifies whether the website is genuine or a phishing website. If the website is phishing website then it can't display the image for a user. The intruder can't enter into the system even if he knows the username.

REFERENCES

[1] Shital B. Patil, Uma Nagaraj "A Novel Anti Phishing Framework Based On Visual Cryptography ", International Journal of Advance Foundation and Research in Science and Engineering (IJAFRSE) Volume 1, Issue 1, June 2014.
[2] K.A.Aravind, R.MuthuVenkataKrishnan, Anti-phishing framework for banking based on visual cryptography, IJCSMA, Vol. 2, Issue 1, Jan 2014, pg.121-126.
[3] Nisha S, Dr.A.Nella Madheshwari, "Secured authentication for internet voting in corporate companies to prevent phishing attacks"
[4] U.Naresh1 U.Vidya Sagar2 C.V. Madhusudan Reddy3, "Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 3 (Sep. - Oct. 2013), PP 28-36
[5] Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu, "An Antiphishing Strategy Based on Visual Similarity Assessment", IEEE Internet Computing, v 10, n 2, p 58-65, March/April 2006.
[6] M.Naor and A. Shamir "Visual cryptography" in Proc. EUROCRYPT, 1994, pp. 1–12.
[7] Sougata Mandal, Sankar Das, Asoke Nath, "Data Hiding and Retrieval using Visual Cryptography" International Journal of Innovative Research in Advanced Engineering (IJIRAE) Volume 1 Issue 1 (April 2014)
[8] Mayur Patil, Vijay Pimplodkar, Anuja R.Zade, Vinit Vibhute, Ratnakar Ghadge, "Survey on Voting system techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3
[9] Ms.BhawnaShrivas, Prof.Shweta Yadav, A Survey on Visual Cryptography Techniques and their Applications, International Journal of Computer Science and Information Technologies, Vol. 6 (2), 2015, 1076-1079.
[10] Abdalla Al-Ameen and Samani Talab "The Technical Feasiblity and Security of E-Voting", The International Arab Journal of Information Technology, Vol.10, No.4, July 2013, p.no.397-404.