International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1596-1600 www.ijaem.net ISSN: 2395-5252

Detection of cyber phishing attack on online voting system using visual cryptography

[1]Ashwini K, [2] Brinda Ramesh, [3]Holachi Tejaswini
[1, 2, 3] *Student Jyothy Institute of technology, Banglore*
Prof. Rakshatha S, Jyothy institute of technology, Banglore

Submitted: 15-07-2022 Revised: 27-07-2022 Accepted: 29-07-2022

ABSTRACT: The online voting application starts by displaying a home page which provides information about how an online voting works to the users of our application. The users need to register before casting their votes. The registration process is managed by the admin. The users need to be logged on to the appslication in order to view and cast their votes for the elections taking place on that particular day. The users can now view all the details of the elections which took place through our application. On click of election ID, the users can obtain information about candidates contesting in that particular election. If the user wishes to cast his vote for a candidate, they can register as a voter by clicking on register to vote. The user who has now registered as a voter will receive the encrypted image of his password from the admin. The images which are provided as a password to the voters is randomly picked and then used for the process of encryption.

KEYWORDS: Verification, Online voting, Website forgery, Cyber security, Phishing attack.

I. INTRODUCTION

Voting is a method for a group, such as a meeting or an electorate, in order to make a collective decision or express an opinion usually following discussions, debates or election campaigns. Democracies elect holders of high office by voting. Residents of a place represented by an elected official are called "constituents", and those constituents who cast a ballot for their chosen candidate are called "voters". There are different systems for collecting votes, but while many of the systems used in decision-making can also be used as electoral systems, any which cater for proportional representation can only be used in elections.

Electronic voting (also known as e-voting) is voting that uses electronic means to either aid or take care of casting and counting ballots. Depending on the particular implementation, evoting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results.

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image. One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography, and using opaque sheets but illuminating them by multiple sets of identical illumination patterns under the recording of only one single-pixel detector.

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. There are two challenges to online voting system which can be seen as well technological as culture:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1596-1600 www.ijaem.net ISSN: 2395-5252

• You cannot at the same time have verifiability of an election and anonymous voting

• Accessibility has to be always guaranteed Identity theft continues to be a problem in voting system across the globe. In computing, phishing is an attempt to criminally acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity. Phishing is typically carried out by email or instant message (IM), although sometimes phone contact is attempted; the phisher often directs users to enter details at a website. Phishing is an example of social engineering. Therefore the problem confronting the study is the prevention of phishing attacks in voting system using virtual cryptography.

II. RELATED WORK

[1].The confidentiality of the election is maintained by applying the appropriate security measures so that the voter can vote for any participating candidate but only if he logs into thesystem by entering the correct password which is generated by merging the two shares using Visual Cryptography scheme. The administrator is responsible for sending the shares, 1st share to voter email id before election and 2nd share will be available in the Voting System for his login during election. The voters get the secret password to cast his vote by the combination of share 1 and share 2 using Voting Cryptography.

[2].They reframe the online voting system to prevent such phishing attacks based on Visual Cryptography (VC) which goals at providing a capability to cast poll for confidential and critical commercial assessments. The system allows the users to cast their vote from any remote location in a fully confidential and secure manner so that the casted vote reaches to the participating candidate correctly. When the voter logs into to the voting system, needs to enter a password, generated by the system by combining the two parts of VC methodology. The first part of the password will be sent to the voters registered email id before the election, while the second part of the password will be generated the voting device. The voter needs to enter the combined password during the voting process to cast his vote. The system is been tested with various known phishing attacks and results are obtained as forecasted.

[3].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.

[4].They have proposed an online voting method that makes use of the internet, because the risk of cheating/threats is growing by the day. Phishing attacks are one such issue that might cause authentication issues. As a result, we've built a secure online voting system based on Visual Cryptography (VC), with the goal of allowing employees to vote on important and private internal corporate decisions.

[5].They have proposed an online voting system that make use of internet, the possibility of cheating/threats has been increasing day by day. One such problem is phishing attack which can create problems in authentication. So, we have implemented secured online voting system using Visual Cryptography (VC) aims at providing a facility to cast vote for critical and confidential internal corporate decisions.

[6].They have proposed one advanced mechanism which will use the joint approach of Face Detection and visual cryptography, to provide more suitable online voting system, through which the voting system will be more efficient, user friendly and will have higher security.

[7].In this paper Open Redirection method is used so that the user is not redirected to any other phished website. Internet voting focuses on security, privacy, and secrecy issues, as well as challenges for stakeholder involvement and observation of the process. A new approach is proposed for voting system to prevent phishing attacks.

III. PROPOSED METHOD

- Encryption process

Encryption is a process which transforms the original information into an unrecognizable form. This new form of the message is entirely different from the original message. That's why a hacker is not able to read the data as senders use an

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1596-1600 www.ijaem.net ISSN: 2395-5252

encryption algorithm. Encryption is usually done using key algorithms. Data is encrypted to make it safe from stealing. However, many known companies also encrypt data to keep their trade secret from their competitors.

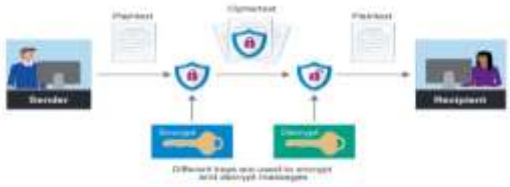

Fig 1.Overview of Encryption and decryption process

The process of encryption is carried out by the selection of a random image that is provided to the voter as their password. Then we perform a bitwise xor operation with the selected image and the key which is randomly generated. Each pixel of the image undergoes a xor operation with the key which is stored in the form of a text file. After the completion his process the encrypted image is obtained.

The encrypted image is sent to the voter when he registers for voting. The Voter then selects election to which he would like to cast his vote. Now the voter is requested to upload the encrypted image which is shared by the admin.

- Decryption process

Decrypted image is now compared with the original image. This is done using jim library and the hash function. If the decrypted image is match with the original image then the voter can cast his voter, the voter will not be allowed to cast his vote until the images match.

Jimp is a node module used to do image processing which is provided by the npm installer. The Jimp – Javascript Image Manipulation Program is a library written entirely in JavaScript for Node, without any external or native dependencies.

Various Image manipulations options available in this library are blit, blur, color, contain and many more.

Image types supported by Jimp:

- @jimp/jpeg
- @jimp/png
- @jimp/bmp
- @jimp/tiff
- @jimp/gif

Nodejs syntax is easy to handle and people with background from Python or C++ can get easily used to it. The compilation time in nodejs is faster than any other. Image hashing (also called perceptual hashing) is the process of constructing a hash value based on the visual contents of an image. We use image hashing for CBIR, near-duplicate detection, and reverse image search engines. Image hashing or perceptual hashing is the process of

- Examining the contents of an image.
- Constructing a hash value that uniquely identifies an input image based on the contents of an image.

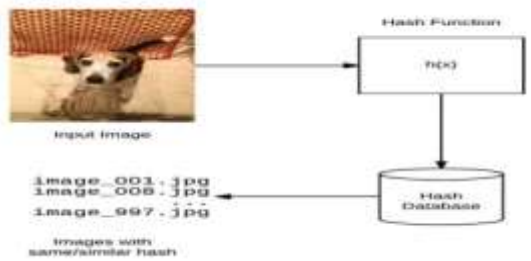

Fig 2. Process of Hash Function

IV. RESULTS

The given below image is used for an encryption and decryption purpose

Fig 3. Image before encryption and decryption

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 1596-1600 www.ijaem.net ISSN: 2395-5252

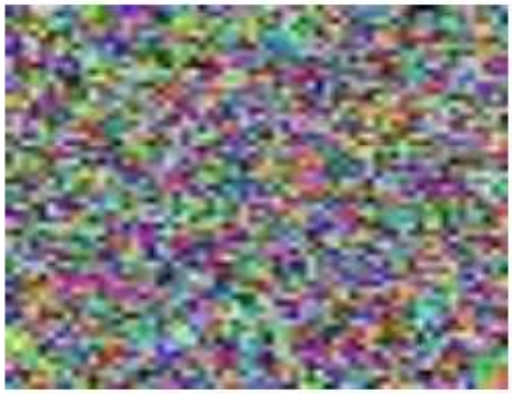

Fig 4. Image after encryption

Fig 5. Image after decryption

V. CONCLUSION

A prominent survey on the voting systems along with the visual cryptography techniques have been kept in mind so as to get the accurate figure of the progression in the field. The growth towards the VC is very high but each and every author explains a different type and the way by which there can be a proper online voting system. According to me the simple way and also an effective way should be carried out and in the future phase of research there can be a comparative study in accordance to the percentage of success rate and the failure rate that can be calculated. This is the proper elaborated study that is done in respect to a few articles, papers and special editions that are released towards the interest of online voting with the concept of VC.

Any democratic nation must understand the importance of elections. Since a small percentage of our countrymen work abroad and are unable to vote in their home country, if this idea were to become law, the voting percentage would increase even more. The online voting mechanism is accessible to such individuals as well as to the elderly and physically challenged. The usage of Visual Cryptography Technique makes it possible for users to quickly determine whether they are on a legitimate website or a phishing site. Voters will find the proposed online voting mechanism to be highly handy.

REFERENCES

[1]. Akshada Tingare, Pragati Shitole, Mohini Raykar, Priyanka Pathare, Prof. Vandana Chavan, "Prevention of Phishing Attacks on Online Voting System Using Visual Cryptography", International Journal of Scientific Research in Science and Technology (IJSRST), Print ISSN: 2395-6011, Online ISSN: 2395-602X, Volume 5, Issue 8, pp.198- 206, November-December-2020.

[2]. Nikitha Kaveriappa, Dr. R. Aparna, Visual Cryptography Based Phishing Suppression for Online Voting System, International Journal of New Technology and Research (IJNTR) ISSN: 2454-4116, Volume-6, Issue-10, October 2020.

[3]. Ramya. R. Nelli, Rashi Mehra, Pallavi Madri, Monica S, Rajeshwari J, 2017, Anti-Phishing I-Voting System using Visual Cryptography, International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 6, Issue 5, May 2017.

[4]. Amisha Singh, Nandini.S, Pawana.S,Supriya.C, Dr.Prakash Biswagar, Prevention of Phishing Attacks on Online Voting using Visual Cryptography, Journal of University of Shanghai for Science and Technology ISSN: 1007-6735.

[5]. Vaibhavi Vitthal Kulakarni, T S Kusuma Sri, Asst Prof. Tahir Naquash H B, 2019, Prevention of Phishing Attack in Online Voting System by using Visual Cryptography, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) RTESIT – 2019 (VOLUME 7 – ISSUE 08).

[6]. Achal Kamdi, Mamta Kamble, Vijaya Tayade, Jeevan Dharne, Rajeev n. Verma,

2017, A novel approach for online voting system using visual cryptography and face detection, International Journal of Advances in Electronics and Computer Science ISSN: 2393-2835 Volume-4, Issue-4, Aprl.-2017.

[7]. Manoj Sabnis, Manisha Bahrani , Bhavna Bajaj, Payal Popat, Prevention of Phishing Attack on Online Voting System, Prevention of Phishing Attack on Online Voting System, Volume 8 Issue No.4.