AVOIDING PHISHING ATTACKS WITH VISUAL CRYPTOGRAPHY

[1]Ketaki Adwait Phansalkar, [2]Saloni Sunil Rane, [3]Mayuri Yashvant Shinde
[1]TE student, [2]TE student, [3]TE student
[1,2,3]Information Technology Engineering,
[1,2,3]Finolex Academy of Management and Technology, Ratnagiri, India

Abstract: Voting system Using Visual Cryptography (VC) aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow casting of vote from any remote place. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct password which is generated by merging the two images using VC scheme. Administrator sends image 1 to voter e-mail id before election and image 2 will be available in the voting system for his login during election. Voter will get the secret password to cast his vote by combining image 1 and image 2 using VC. Phishing is an attempt by an individual or a group to get personal confidential information from unsuspecting victims. Fake websites which appear very similar to the original ones are being hosted to achieve this. 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.

***IndexTerms* – Visual Cryptography, Captcha, Phishing attack.**

I.INTRODUCTION

Voting system is the pillar of every democracy in which voters choose their leaders. Voting scheme have grown from counting votes manually in previous days with the help of electronic voting machine. This offline voting system is time consuming and less secure process. Also maximum people cannot vote because of their busy schedule.

The main idea behind secure online voting system is to overcome the drawbacks of offline as well as the current online voting system. Also it will reduce the paperwork, time, also the damage of electronic machine, etc. Secure online voting system is the system through which any voter can vote from anywhere in country.

Phishing attack is a type of attack in which a malicious user will create a fake website as similar to original website to get the information of voter. Also visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that the decrypted information appears as a visual image.

Our main goal is to prevent phishing attack on online voting system using visual cryptography to overcome the drawbacks of existing voting system.

II.LITERATURE SURVEY

2.1) Online voting system using biometric verification

2.1.1) Features:

This paper gives the information about the system which is completely automated, unbiased and online for easing the process of voting, increasing security and reducing the counting time. The system is divided into two sections those are voter registration section and actual voting section. In the voter registration process the data of the voter will be saved in the repository including the voters unique identification number and finger prints information. During actual voting the user will be verified with the help of a biometric device. The biometric device checks the information of the user saved in repository by wifi communication and if the user is authenticated the user is approved to vote. This system is easy to implement and easy to use[1].

2.1.2) Disadvantages:

1) In present day scenario, EVM results can be tampered by the program stored in EVM and by installing a look alike component which can be instructed to tamper results.
2) Errors are part of all human beings; it is very unlikely for humans to be 100% efficient in data entry.
3) The anonymity of the voter is preserved and there is no way to link the voter to the vote casted by the voter.

2.2) An efficient and securable online voting system

2.2.1) Features:

An online voting system which involves the procedures like registration of voters, vote casting, vote Counting and declaring the results would constitute a good solution to replace current system and the proposed system in this gives the information about their own system or arranged by government the system contains different methods for voting like electronic voting which helps the voters to cast votes in an electronic way means in computerized equipment. The system also includes the computer in which electronic voting machines looking like ATM or personal computers used to cast the votes by touch screen or a pointer.

2.2.2) Disadvantages:

1) The process of collecting data and entering the data into database takes too much time and is expensive to conduct.
2) The process involves too much paper work and paper storage.
3) The system is totally insecure as malicious user can easily attack by doing any changes throughout the system.

2.3) Title: Online voting system using mobile

2.3.1) Features:

The traditional voting system can be changed to a newer and effective approach termed as mobile voting. The mobile voting system provides the convenient, easy and efficient way to vote eliminating the shortcoming a traditional approach. In this paper the proposed to build the E- voting system which is basically an online voting system through the smart phones or website. To achieve the security they are using One time password (OTP) principle. The system can be used anytime and from anywhere by the voters. No one can cast votes on behalf of others and multiple votes. It saves time and having unique identification by using aadhar card or voter id.

2.3.2) Disadvantages:

1) There is no documentary evidence and tangible results for election.
2) It is possible for hackers to access and modify the results after getting any user id

III) Types of Security attack

Before designing this system we studied different attacks which can be done on the voting system. The attacks are as follows-

A. Phishing Attack
Phishing attack is a technique in which the malicious user can create a fake website as similar to the original website to get information of voter.

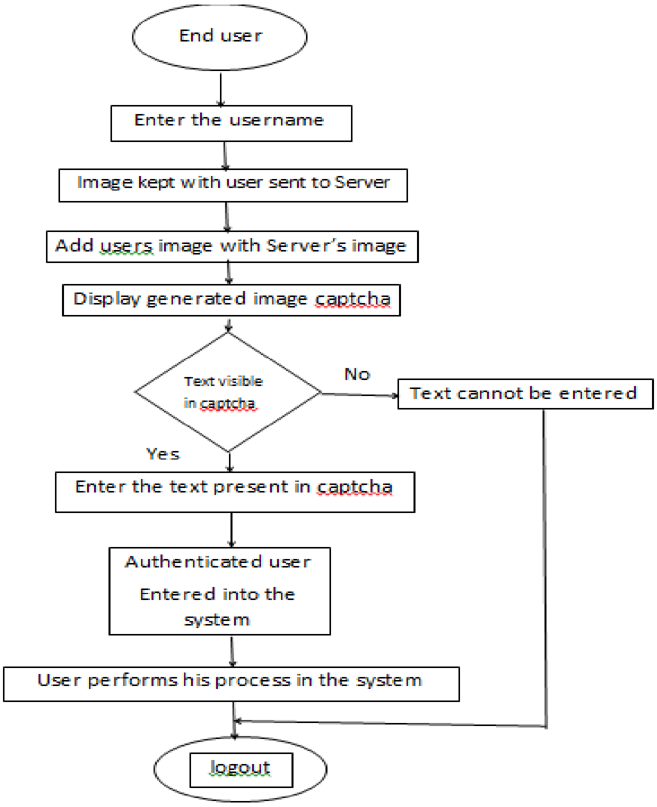
B. Pharming Attack
In pharming attack malicious user will redirect the original website

C. SQL injection
In this malicious user will destroy all the database of original website by using sql query.

D. Password Attack
Password attacks can be implemented using several methods, including brute-force attacks, Trojan horse programs, IP spoofing, key loggers, packet sniffers, and dictionary attacks. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both. These repeated attempts are called brute force attacks.

E. Man in the middle Attack
A complex form of IP spoofing is called 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.

IV.PROPOSED ONLINE VOTING SYSTEM


End user
Enter the username
Image kept with user sent to Server
Add users image with Server's image
Display generated image captcha
Text visible in captcha
No
Text cannot be entered
Yes
Enter the text present in captcha
Authenticated user Entered into the system
User performs his process in the system
logout

In this system, firstly the phishing detection will be done as explained in section 3. The prevention will be done in the system as show in the figure.The voting process will be divided into two phase. First the registration phase and then the actual voting phase. In the registration phase, the image will divided into two halves and shared between the user and the server. During voting phase, the user will enter its username. The part of the image kept withe the user will be sent to server. This user's part will be added with server's image and generated captcha image will be displayed. If the text is visible in captcha then the user is an authenticated user and he/she is allowed to enter the system by entering the text in captcha. Else if the text is not visible then the text in captcha cannot be entered and user cannot enter the system.

V. CONCLUSION

Voting plays an important role for any democratic country. If this proposed system is implemented, then the voter does not have to go to the voting center. This system is very useful for those peoples who are living in another countries also for the peoples who are physically disabled. Since Visual Cryptography Technique is used, user can able to find out whether he is in phishing site or original site easily. Proposed online voting system is very effective and it will useful for voters and organization in many ways and it will reduce the cost and time.HJJJJKK

VI. REFERENCES

[1] Network Security, https://en.wikipedia.org/wiki/Network_security, accessed on May 2015.

[2] Joey Paquet, http://users.encs.concordia.ca/~paquet/wiki/index.php?title=Capability_ maturity_model, accessed on May 2015.

[3] Implementation of Electronic Voting System In Mobile Phones With Android Operating ,ISSN 2079-8407,Volume-4,Number9,Sept-2013,JETCIS.

[4] 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.

[5] The Design of Web Based Secure Internet Voting for Corporate Election, ISSN 2319-7064, Volume-2, Issue-7, July-2013, and IJSR.

[6] An Efficient Online Voting System, ISSN 2249-6645, Volume-2, Issue, July-Aug-2012, IJMER.

[7] Villafiorita A, Weldermariam K, Tiella R, “Development, Formal verification and evaluation of an e-voting system with VVPAT”, IEEE Transactions on Information Forensics and Security, 2009, p.no. 651661.