Prevention of Phishing Attacks on Online Voting using Visual Cryptography

[1]Amisha Singh, [2]Nandini.S, [3]Pawana.S,[4]Supriya.C, [5]Dr.Prakash Biswagar
B.E Student, Department of Electronics and Communication Engineering, R.V. College of Engineering, Bangalore [1][2][3][4],Professor, Department of Electronics and Communication Engineering[5] [1]amishasingh.ec17@rvce.edu.in,[2] nandinis.ec17@rvce.edu.in, [3]pawanas.ec17@rvce.edu.in,[4]]supriyac.ec17@rvce.edu.in [5] prakashbiswagar@rvce.edu.in

Abstract— According to the report, due to their busy schedules, only a small percentage of people vote. There are numerous causes; for example, everyone may be required to go to a polling centre, where they will be required to stand in a long line and will be exhausted due to their tight schedule. As a result, we've 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.

.Index Terms—Authentication, cryptography, phishing, online voting.

I. INTRODUCTION

Voting is the basis of any democracy. To keep democracy healthy, voting process must be secure and reliable. With traditional voting system it is not possible to vote from anywhere at convenient time. You have to physically go to voting centre, wait in queue, and then finally cast your vote. There is lack of vote-cast verifiability which cause loss of trust of voters. Low voter turnout is a result of this unappealing, time-consuming process. It is extremely difficult to hold elections in the midst of a pandemic, such as COVID 19, by forcing voters to queue and vote.

The Internet has ushered in a new era. Many things, such as payments and businesses, are moving online. Voting will be considerably easier using the online voting system. People can vote from any location. There will be no need to wait in line for your turn, so the process will be quick. This will motivate a big number of people to vote.

E-voting is also more expensive than traditional voting systems. Physical security is an inherent expense of voting on ballot paper or with an EVM machine. Human resources are heavily utilised in the implementation of these systems. There is also the possibility of human error during vote tallying owing to human participation. Many ideas have already been offered in an attempt to build a secure online voting system. The e-voting technology that we propose will help to reduce election costs. Because everything is automated, the odds of making a mistake are none. To make the voting system secure and reliable, cryptographic and steganographic technologies are applied. The privacy of the voter and his vote are accorded top priority.

Visual Cryptography (VC) voting system seeks to provide a tool for casting votes for sensitive and confidential internal corporate decisions. It has the capability of allowing voters to vote from anywhere in the world. The election is held in complete secrecy, with sufficient security mechanisms in place to allow voters to vote for any participating candidate only if they connect into the system with the correct password, which is generated by combining the two shares using the VC technique. Before the election, the administrator sends share 1 to the voter's e-mail address, and share 2 is available in the voting system for his login during the election. By combining share 1 and share 2 with VC [1], the voter will receive the secret password to cast his vote.

Phishing is a technique used by an individual or a group to get personal information from unwitting victims. To do this, fake websites that look quite similar to the actual ones are hosted. Internet voting focuses on issues of security, privacy, and secrecy, as well as problems for stakeholder participation and process observation. To combat phishing attempts, a new voting system technique is offered. 1st

OBJECTIVES

- To create a full stack web application.
- To create a secure and reliable online voting system.
- To provide service to create, conduct election and declare the result

II. METHODOLOGY

The literature review is finished, and the objectives have been set. An acceptable algorithm is chosen during the literature review. To protect data from hackers, information

security techniques such as Steganography, Cryptography, and other encryption techniques have been developed. Steganography techniques can be applied to any type of digital media, including text, video, audio, and photographs. Visual cryptography and Secret Image Sharing are cryptographic techniques for safeguarding data such as written documents, textual images, and handwritten notes.

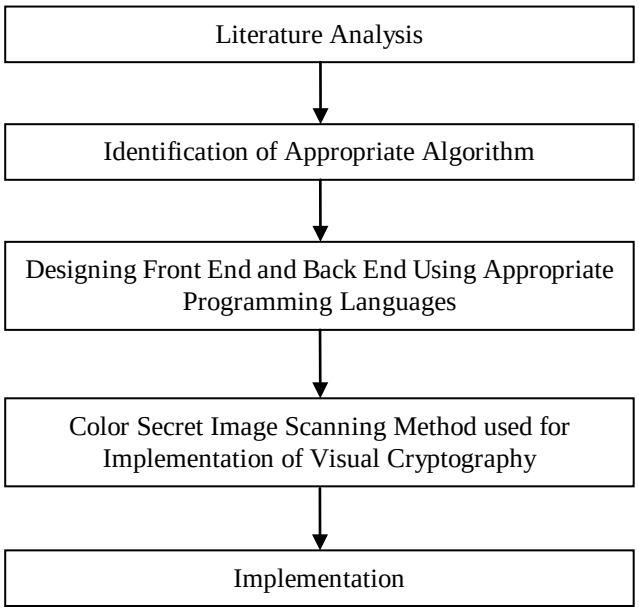


Figure 1: Methodology flow chart

The front end and the back end design is done using appropriate language. Steganography techniques/Visual cryptography and Secret Image Sharing are cryptography techniques are utilized for the purpose of securing the personal information such as password, secret code, etc. Finally, the design is implemented and the results are analyzed.

III. IMPLEMENTATION

The system architecture is depicted in Figure 2. As the figure shows that

- The browser interacts with http server to provide necessary functions.
- An e-ballot is generated for voter using steganography to cast his vote.
- This vote is counted at application server using database server and further encrypted using visual cryptography.
- The user receives one share generated via visual cryptography, while the second share is stored on the database server.
- User can upload his share to create vote cast receipt. (The receipt does not contain information about to whom the vote was given).

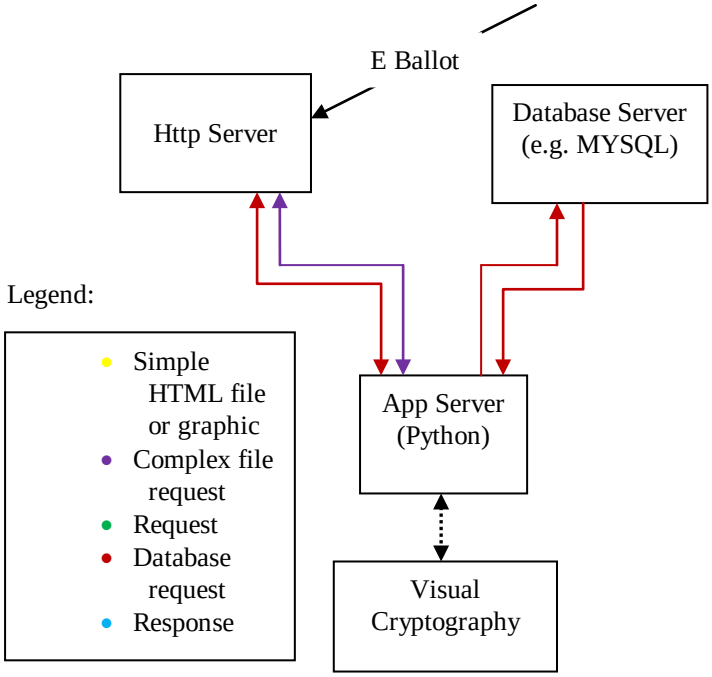


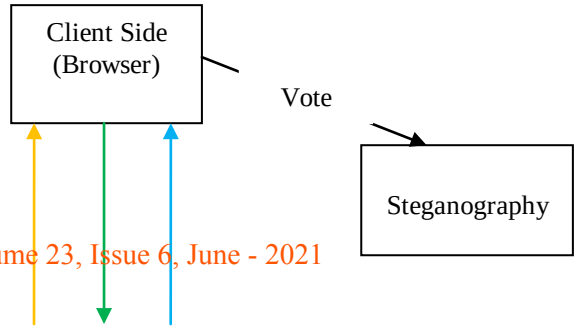
Figure 2: System Architecture

This section describes the implementation details of E-Vote System.

- Static features of front end of Secure E-Vote System is implemented using HTML,CSS (with bootstrap).
- Dynamic features of the system are implemented with Javascript.
- Backend is implemented using Python. Code for Steganography and Visual Cryptography are written in python.
- For this system, SQLite database is used.
- This website is supported by Javascript supporting browsers like Chrome, Firefox etc.

Functions:

- Create Election – Administrator will be able to create an election.
- Add election candidates – Administrator will be able to add candidates for the election.
- Add polling officers – Administrator will be able to add polling officers.
- Add eligible voters – Polling officers will add eligible voters.
- Authenticate voters – System will authenticate voters using username and password to login.
- Vote – Voters will be able to vote only once through their login.



- Steganographic encryption – Steganographic encryption will be used to transfer vote from browser to e-vote server.
- Visual encryption and decryption will be used to create vote receipt service for verifiability.

- Real time Vote statistics display to administrator.
- Results of election will be declared on the day of result using threshold encryption cryptography.

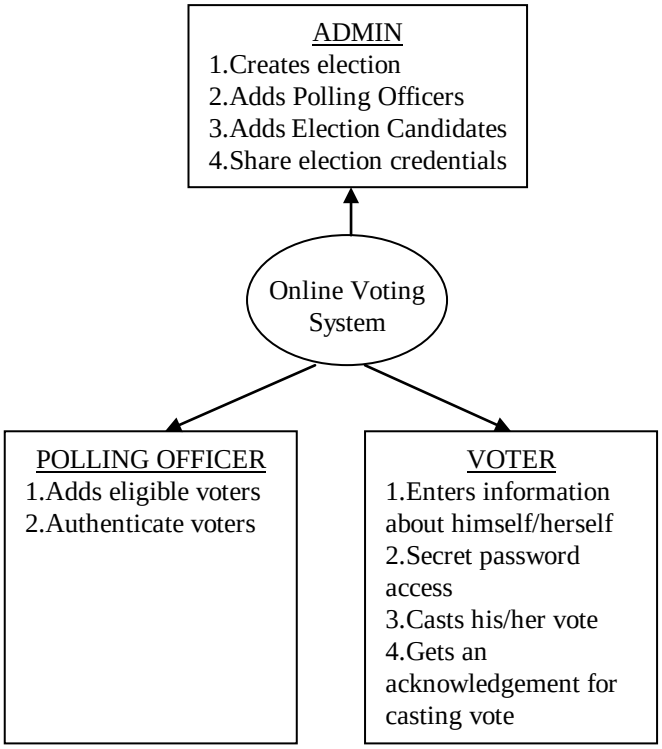


Figure 3: Context diagram of online voting system

IV. RESULTS

The Figure 4 shows the home page of Secured E-Vote system. The admin login takes place.

Figure 4: Home page of Secured E-Vote system

The admin creates the election by entering the election start date and end date which is depicted in Figure 5.

Figure 5: Create election

The admin adds the Polling Officers and election candidates which is shown in Figure 6.

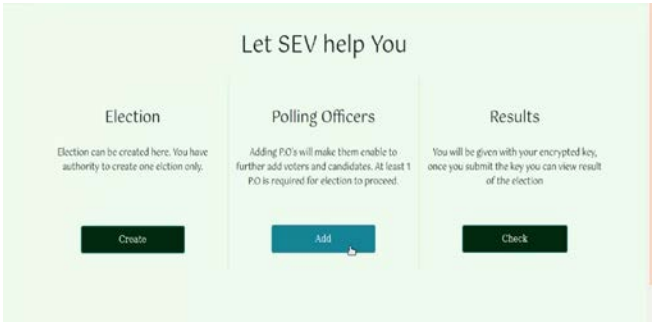


Figure 6: Admin page (Through which election is created, polling officers are added and the election results are viewed)

The polling officer adds eligible voters by entering their details as shown in the Figure 7.

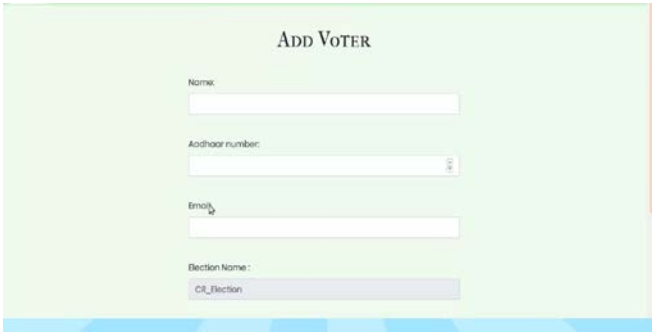


Figure 7: Voter's details

The voter gets a notification about the election as soon as his/her name is added to the voter's list. The voter logins to the E-Voting portal using the credentials sent to him/her. The voter gets an access of the secret password and casts his/her vote.

Figure 8: Secret password access using Visual Cryptography

Once the voter is done with casting his/her vote, he/she is not allowed to vote again which is depicted in Figure 9.

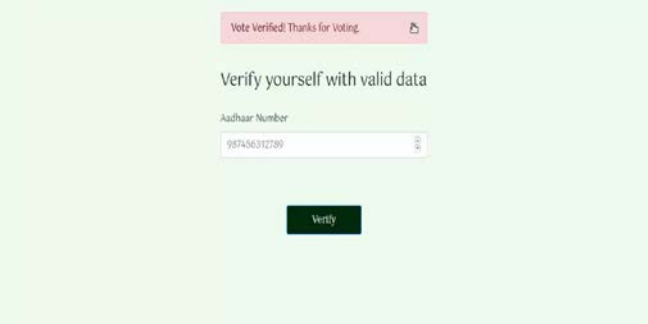


Figure 9: Validation/verification of vote casted

The admin/polling officer keep monitoring the status of the election and at the end the results are announced as shown in Figure 10.

Figure 10: Status of the election

V. CONCLUSION

The Secure E-Vote system demonstrates that a secure voting service may be provided via Internet. Secure E-Vote offers the potential to cut election costs. This applies to both financial and human resources. This system's efficiency is demonstrated by its fair and limited use of resources. The Secure E-Vote System offers an elegant yet simple voting system. Result of ”User acceptance” testing support these conclusions. The scope of this system is limited to elections within an organisation.

VI. REFERENCES

[1] S. Nisha and A. N. Madheswari, "Prevention of phishing attacks in voting system using visual cryptography," *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, India, 2016, pp. 1-4, doi: 10.1109/ICETETS.2016.7603013.

[2] 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) .

[3] E-voting software, CS 312 Project, Software Requirements Specification (SRS) Document by Anurag, Ashish, Harshavardhan, Ramkrishan, Sumesh, 2018

[4] Anti-Phishing Working Group, Global Phishing Survey: Trends and Domain name use in 1H2009, 2009Anti-Phishing Working group. http://www.antiphishing.org/., 2009

[5] Anti-Phishing Working Group (APWG), Phishing activity trends report for the month of June, 2007 http://www.antiphishing.org, 2007

[6] Dhamija, R. and Tygar, J. D. 2005. The battle againstphishing: Dynamic Security Skins. In Proceedings of the2005 Symposium on Usable Privacy and Security, SOUPS '05, vol. 93, ACM Press, 2005

AUTHORS PROFILE

First Author
Amisha Singh
B.E in Electronics and Communication Engineering,
R.V. College of Engineering
Bangalore.

Second Author
Nandini.S
B.E in Electronics and Communication Engineering,
R.V. College of Engineering
Bangalore.

Third Author
Pawana.S
B.E in Electronics and Communication Engineering,
R.V. College of Engineering,
Bangalore.

Fourth Author
Supriya.C
B.E in Electronics and Communication Engineering,
R.V. College of Engineering
Bangalore.

Fifth Author
Dr.Prakash Biswagar
Professor, Department of Electronics and Communication Engineering,
R.V. College of Engineering, Bangalore.
Education qualification : B.E (Electronics)
M.Tech.(Industrial Electronics)
Ph.D (Smart antennas)
Experience : 30 years (Teaching)
10 months (Industry)
Area of interest : Communication Systems.