Avoiding Phishing Attack on Online Voting System Using Visual Cryptography

Amal K Tom[1]

[1]Student, Dept. Of Computer Science & Engineering,
Mangalam College of Engineering, India

Arshad Aboobaker[2]

[2]Student, Dept. Of Computer Science & Engineering,
Mangalam College of Engineering, India

Ebin Baby[3]

[3]Student, Dept. Of Computer Science & Engineering,
Mangalam College of Engineering, India,

Aishwarya Mohan[4]

[3]Assistant Professor, Dept. Of Computer Science & Engineering,
Mangalam College of Engineering, India,

Abstract ~ **Visual cryptography is mostly used in voting systems to provide the option of casting vote for internal organizational decisions. It is adaptable enough to cast votes from a distance, places. Elections are conducted in the strictest of secrecy and are entirely private. To allow members to vote using their computers and laptops, we have suggested an online voting mechanism for the Maharashtra Carrom Association. We use CAPTCHA code and Image Share technology to protect security. The suggested solution gives voter anonymity while maintaining the privacy of votes, transparency, and security of the election.**

Keywords: visual cryptography, phishing, CAPTCHA

I. INTRODUCTION

Elections are the foundation of a democracy, so fairness is crucial. Voting is the only method to decide who will represent you. For people who are elderly, live far from their houses, or are in a remote area, voting in a traditional election requires them to travel to a polling place and cast their ballot. Through the internet, voters can cast their ballots for their MPs from any location. Cryptography is used in the online voting method. This guarantees an effective and secure method of counting votes. Making a voting system on the internet has many challenges to overcome. Some major issues are voting in a secure manner and accompanying many voters. There are some internet voting systems that cannot work in situations with many voters. Our proposal uses visual cryptography to overcome these issues. Everywhere there are elections, voters must cast their ballots in a polling place. The process of casting a vote is extremely complicated and involves many steps. Numerous plans need to be made. It requires a lot of manual labour. Voting in this organization requires voter presence at voting location. As a result, the goal is to ensure that voting is efficient and secure. Voting becomes more secure thanks to visual cryptography [8]. It is crucial to implement these technologies since they will cut labour requirements and improve voting efficiency. Visual cryptography is a very safe method used for privacy that enables the encryption of secret images or data by sending it to a secure share and allows the decryption to be completed without the use of any computing devices. An image is separated into shares using visual cryptography, a secure sharing technique. Only after stacking a sufficient number of shares will the information regarding the original photocopy (Voter Password) be acknowledged. To authenticate the system in the suggested method, we employ a visual cryptographic strategy called the Internet Voting System (IVS) using 2-out-of-2 Visual Cryptography (VC). The voter's email address is shared with another password; thus the hacker cannot access it in this approach. The voting system is greatly in need of the two-way security that electronic voting offers. The voter decodes the message by piling up the shares one after another. A secret image S (voter password) is encoded into a set of shadow images called shares for P participants, with participant P receiving one share. Participants' shares must be stacked one on top of the other before the image can be retrieved. The voter's email address is shared with another password; thus the hacker cannot access it in this approach. The voting system is greatly in need of the two-way security that electronic voting offers. The voter decodes the message by piling up the shares one after another. A secret image S (voter password) is encoded into a set of shadow images called shares for P participants, with participant P receiving one share. Participants' shares must be stacked one on top of the other before the image can be retrieved.

II. EXISTING SYSTEM

Types of voting system

Three different voting systems are now accessible. We are focusing on the online voting system as a result of studying this voting system.

A. Paper ballot system

Paper ballot system is used in old days for voting. Ballot is used by each voter and ballots are not shared. Depending on the type of voting system different ballots may be used. Ranked ballots is the type of ballot system which allow voters to rank candidates in order of preference, while ballots for first-past-the-post systems only allow voters to select one candidate for each position.

B. Electronic voting system

The term "e-voting system" also refers to an electronic voting system. E-voting may use an electronic voting system, depending on the specific implementation. There are two primary forms of electronic voting: in-person electronic voting under the actual supervision of officials from governmental or independent electoral authority, and distant electronic voting over the Internet.
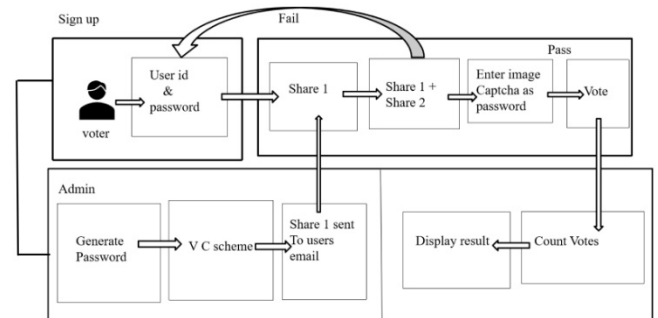
C. Online voting system

Online voting is a novel method that allows voters to cast their ballots at any time and from any location. After registering and giving the system their personal information, voters can vote by logging in to the system and undergoing verification.

III. PROPOSED SYSTEM

Think about using an online voting mechanism to choose the president or any other association for carrom power. All members are registered at the time of the association election by providing their personal information. Cryptography is a regularly utilized method in electronic voting because it provides a strong protection against threats. Cryptography is a regularly utilized method in electronic voting because it provides a strong protection against threats. Numerous plans have been developed and proposed in order to guarantee the integrity of an election.

Cryptography is employed in these techniques to secure the data transmission between the voter and the server, preventing data leakage to a third party. In order to protect the privacy of voters, the integrity of the ballots cast and collected, the validity of the results, and the authenticity of the voter, encryption techniques are also used in every step of the system. There are numerous cryptography techniques that can be used, including blind signature schemes, homomorphic encryption, oblivious signature schemes, bit commitment schemes, Schnorr identification schemes, mixed-net schemes, digital signature schemes, secure multi-party computation, cryptographic hash functions, etc....

As the image shown below, the voter will share an image with the system at registration, which will then split it into two parts.

The first component (SHARE1) will then be transformed into a password using the VC technique and sent to the voter's email address. The server retains the second half of the picture (SHARE2). Voters will then enter into the system using the use rid and password provided by it, and the system will then add SHARE1 and SHARE2 to generate the CAPTCHA code. The voter will be permitted to vote if they can see the CAPTCHA code; else, they won't be able to. The system will tabulate the results after counting the votes. Then Two shares of the CAPTCHA will be distributed. Visual cryptography will be used to create these password sharing. However, the image will first be changed into a monochrome, or black and white, image, before being divided into shares. Access structure will be taken into account while forming shares as well. Access structures are employed to teach students about all the security aspects involved in cooperative resource acquisition we will be encoding the A into n number shares of transparencies. The number of pixels expands as the shares rise. Integer linear programming (ILP) will be used to prevent the modelling of enlarged pixels. This will enable the creation of a simple matrix with the fewest possible pixels. Thus, for the system that needs the fewest shares, an ideal pixel expansion will be accomplished. One share will be sent to the voter using SMTP when the two shares are established. All of the pixels will be divided into small blocks by the shares that are created, with the number of white blocks equaling the number of black blocks. The shares will be combined at the time of voting, and if the user is valid, CAPTCHA will be shown. When a voter is suspected of being malicious, they are immediately logged out of the voting system and are not permitted to cast a vote.
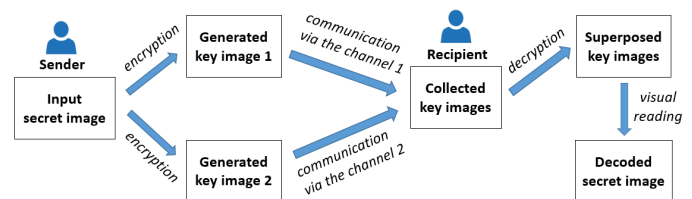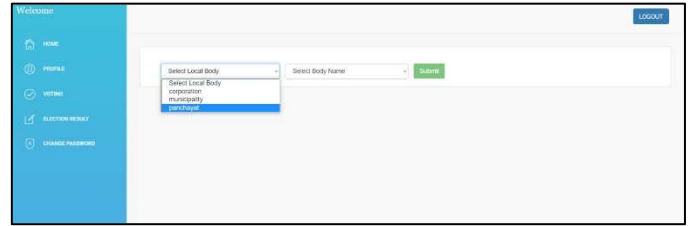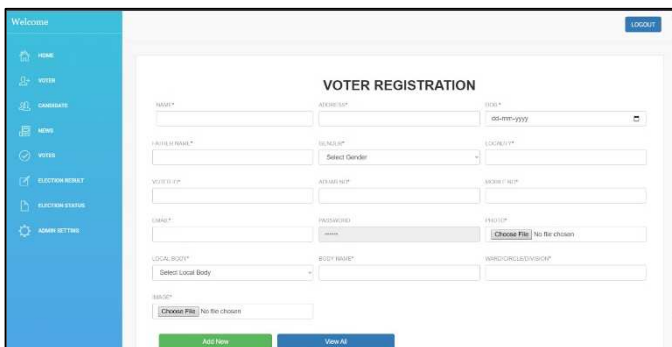
IV. IMPLEMENTATION MODULES

A. Front End Home Page

As shown in fig.2, this is the main page of our online voting system from this page we are going to the next page.
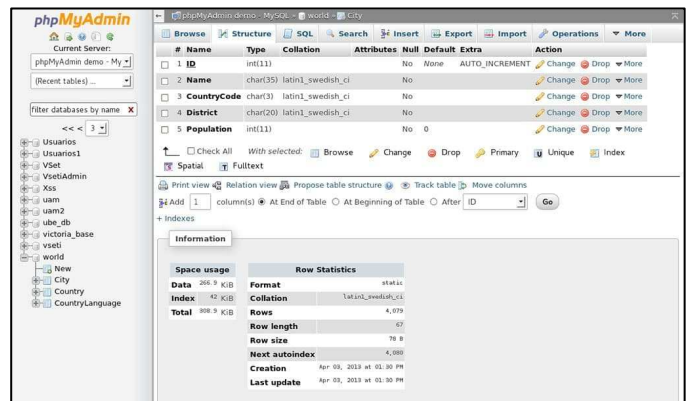

B. Registration Page

On this page, the voter will enter their personal data. The image will also be provided by the voter as a password for voter authentication. Following that, the image will be split into two pieces using a visual cryptography mechanism, with one portion being transmitted to the voter as an authentication key.

C. Login Page

Following registration, the voter logs into the system to cast their ballot using their username and the share of the picture that the system has provided. Voting will be permitted if the voter uploads the correct image, which will just make the CAPTCHA visible.

This is the page where the voter actually selects the best candidate.

E. Backend

When a voter registers, we will save all their information on the back end. This information will be used to distribute the share. Only registered voters will be permitted to log on to the system, and they will all be validated.

V. CONCLUSION

Any Democracy must have voting as a fundamental component. The voter wouldn't need to visit the voting Centre if the proposed system were to be implemented. Both those with physical disabilities and those who reside abroad will find this technique to be of great help. He can quickly tell if he's on a phishing site or the legitimate one thanks to the Visual Cryptography Technique. More people than the traditional voting system have been interested in voting online, especially those who live far from their homes. Due of transparency and security concerns, several academics have recently started to show interest in this topic. . So by studying all the attacks and visual cryptography techniques from different papers we will be designing an efficient voting system that will prevent phishing attack

Special Issue - 2023

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
ICCIDT - 2023 Conference Proceedings

VI. REFERENCES

[1] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2091–2121, 4th Quart, 2013

[2] Avoiding phishing attack with visual cryptography, Prof Atiya Kazi, Ketaki Phansalkar, Saloni Rane, Mayuri Shinde, 2019

[3] Implementation of authenticated and online voting system, IEEE -31661, 2013.

[4] Phishers' Favorites: After Five Quarters, Microsoft is Unseated by PayPal. Accessed: Apr. 12, 2020.

[5] X. Zhang, Y. Zeng, X.-B. Jin, Z.-W. Yan, and G.-G. Geng, "Boosting the phishing detection performance by semantic analysis," in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2017, pp. 1063–1070