A Review on Highly Secure Online Voting System using Cryptography

Barot Kajal[1], Brijesh Vala[2], Warish Patel[3]

Department of Computer Science and Engineering

Parul Institute of Engineering and Technology, Parul University

Email: *190303201002@paruluniversity.ac.in[1], brijesh.vala@paruluniversity.ac.in[2], warishkumar.patel@paruluniversity.ac.in[3]*

DOI:- https://doi.org/10.47531/SC.2022.16

Abstract

These days hardly anyone goes to the polls because of their tight schedule. There are numerous reasons, and some may need to go to the polls, we may need to wait in long lines, many may be drained due to their tight schedules. So we have created a web-based voting system. But this system has some drawbacks. Phishing attackers legally obtain passwords from clients and they go to critical sites with the correct secret passwords. Consider a web-based voting system for corporate organizations, voting once a year to elect a president, secretary, or critical manager. In the current system, every voter has to gather at one place on the Election Day and cast their vote. In this method, we are using another scheme which is known as visual cryptography. In this plan, we are using visual data for security. Here we are dividing the unique picture into two into four which are placed in separate databases. At whatever point these two offers are intertwined with each other, we get the original picture. When we get the original picture, it is used as a secret password. This system is very helpful and acceptable for online remote voting. This system is an electronic application so that the web can evaluate it through any valid personal space on the planet.

Keywords: - *Verification, Online voting, Visual Cryptography, Phishing attack, Cyber security, Privacy, Secret password*

INTRODUCTION

Elections are held everywhere. However, voters have to go to the polling station to cast their votes. The political membership process is exceptionally complex, and many things are needed to advance voting. Large arrangements have been made to finish. It involves manual work. Government elections are held by area. The voter must be available to vote at the polling place to cast his vote. This may reduce voter support; Web-based voting simplifies this undertaking. Voting in visual cryptography involves security. It is essential to implement such systems because that reduces labour, make ballet easier to use and more productive. Individuals must be available at the location for selection.

Visual cryptography is a system of encoding pictures. In this system, the client will be contacted to upload a security picture during registration. The customer will receive the security part of the security picture via email. This share will be in an encrypted format. The customer can log in to the system to change the details at any time. Only when voting, the customer must upload a security share. If the share is incorrect, the poll cannot be voted on because the security share is generated using random pixels, so the real picture can't be accurately predicted. Additionally, the share cannot be retrieved by some other client or disapproved person as it will be securely sent via email. Ballet casting will only be fruitful if the correct share relating to that client is uploaded.

Fraud sends fake messages or sets up fake sites that copy. Phishing is a form of identity online identity theft in which fraudsters trick Internet users into submitting personal information to illegal websites. Phishing tricks are usually displayed as spam or pop-up and are constantly challenging to identify. When fraudsters obtain your data, they can use it for all kinds of identity fraud, risking your excellent reputation. Fishers will become more sophisticated in the design of their fake sites. Phishing is the data of the types of fraud, so be comfortable with various phishing tricks for you and figure out how to prepare for it. The most proper and direct way to secure a system asset is to assign it a unique name and a corresponding password.

Cryptography is the study of protecting data. It has been used as a means of safe communication between people and governmental organizations. Today, cryptography is the foundation of advanced security technologies used to secure data and assets on both open and closed networks. Belief is the process of examining the personality of a person or thing. When you confirm something, the purpose is to check that you have a real deal.

When you confirm a person, the objective is to check that you are not allowing an impostor. It is necessary to implement their methods to determine the level of authorization of the application's user. Applications often do this by keeping private records that include the names of customers to whom who has access. Databases applications, for example, regularly maintain private approval tables to control the fields in a record that a specific client can view or modify. There are many types of applications based on the internet.

One of them is the web-based voting system. Few people advocate the benefits it brings, for example, mobility, openness, improved speed and accuracy in delivering ballots from home. The exact number that it represents is concerned about the crisis, for example, inconsistent entry, breach of mystery and ambiguity. And a change in the effect of a political race. The project focuses on preventing phishing attacks and secure authentication of Internet voting systems using visual cryptography. Visual cryptography is a unique encryption strategy to hide data in pictures so that it can be decrypted by human vision if the correct key picture is used.

LITERATURE SURVEY

There are online voting systems from the early days to the current technological development, explained in this paper. Develop voting plans to use ICT resources to provide more efficient voting services than traditional paper-based voting methods. Voters see themselves as consumers, and the government is expected to make the voting business more convenient. Over the past decade,

various forms of electronic voting, in particular, have been attracting considerable attention as additional voting methods for remote voting, political parties, candidates, election administration and most importantly, to make the democratic process more efficient and promising for voters.

Many types of the internet or remote electronic voting systems are applied with varying degrees of success. Although some systems were running well, some were scrapped, some were implemented due to security concerns.

There are three types of voting systems:

1) Paper ballot system

The paper ballot system is the most widely used standard voting system. It will be used before the implementation of the electronic voting system. The paper ballot system consists of paper and sealed ballet. Every voter uses one ballot, and they do not share it. Disadvantages of this system are (i) time consuming; ii) Low telly speed.

2) Electronic voting system

An electronic voting system is a type of voting system that uses electronic ballots to allow voters to relay their secret ballots to election officials over the internet. The disadvantages of this system are: (i) people with poor computer knowledge cannot vote correctly; (ii) sensitive to security threats; (iii) polling station power consumption; and (iv) costs.

3) Online voting system

The online voting system is the latest electronic voting system in which the ballot is transmitted over the internet through a web browser. Voters can vote online from anywhere in the world. The only drawback to using this tool is protection.

There are some security-related issues related to online voting:

Most apps offer a high level of password protection and do not focus on phishing attacks. Through phishing, attackers obtain users' passwords directly, and with the correct password, they can access the appropriate web pages. There is no efficient way to protect website users from phishing.

We developed a secure Internet-based online voting system using an identity-based encryption system to meet the security requirements for the privacy, confidentiality, eligibility, fairness, verification and receipt of online voting.

The main proposal was a more secure online voting protocol to meet the security requirements of privacy, anonymity, eligibility, fairness, verification and the uniqueness of secure online voting.

The requirements of privacy, eligibility, transparency, accuracy and uniqueness for secure e-voting, two billionaire pairs created an identity-based secure online voting system based on cryptographic algorithms.

Comparative Table

Sr. No	Paper Name	Publication Year	Conference/journal	Methodology/tool/ techniques used	Limitations	Future scope
1	A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature	2020	IEEE	Batch verifiability, early voting, elliptic curve cryptography, end-to-end verifiable, functional digital signature, Internet-	Functional digital signature for anonymously issuing a blank ballot to a voter and using the BLS short signature scheme to protect the	The future of voting: End-to-end verifiable internet voting-specification and feasibility study

				voting system.	vote from any modification.	
2	Phish-haven -An Efficient Real-Time AI Phishing URLs Detection System	2020	IEEE	AI-generated phishing URLs, ensemble machine learning, human-crafted phishing URLs, lexical features, multithreading, URL HTML encoding,	Extracts content of web-pages, hence computationally inefficient Non-Proactive approach Requires source codes or the entire page content of the website	Phish-haven can be further enhanced by incorporating unsupervised learning, by applying multithreading techniques at an input unit
3	Avoiding Phishing Attack on Online Voting System Using Visual Cryptography	2020	Springer	Visual Cryptography; CAPTCHA Image	Visual Cryptography Technique used to detect phishing sites or original sites easily.	We will be designing an efficient voting system for Carrom Association that will prevent phishing attacks.
4	Secure Electronic Voting Using a Hybrid Cryptosystem and Steganography	2019	Science direct	SDLC method for design and implementation of voter's information system. This work employed the iterative waterfall model.	Hybrid cryptosystem and steganography were developed to proffer a more robust scheme in fulfilling the security requirements for electronic voting.	The direction of future works can be tuned towards satisfying the information security requirement for availability. Ensuring availability in information systems also involves preventing denial-of-service attacks.
5	A Novel P2P based System with Blockchain for Secured Voting Scheme	2019	IEEE	Blockchain, P2P network, Ethereum, AES, RSA, security	The existing systems and labels some of the issues of e-voting	This proposed system can be further enhanced by replacing OTP verification with fingerprint or face recognition in real time implementation.
6	SeVEP: Secure and Verifiable Electronic Polling System	2019	IEEE	Authentication, efficiency, electronic polling, malware, security, verifiability.	Resource allocation polling systems have authentication, the process of electronic polling.	Develop a working prototype of SeVEP, and evaluate its scalability and usability in a real-world deployment.
7	Towards Developing a Secure and Robust Solution for E-Voting using Blockchain	2019	Springer	Coercion resistance problem, Blockchain, Online Voting process	Developing a secure solution for an online Eelection process information	To solve the coercion resistance problem to solve, cryptographic algorithms.
8	E2E Verifiable Electronic Voting System for Shareholders	2019	IEEE	Electronic voting, Shareholder voting, End-to-end verifiability, Zero-knowledge proofs,	Verifiable election process	The more general case that voters to use a smartphone may depart and leave

				Decisional Diffie Hellman assumption, Security proof.		dynamically within the computation period.
9	An Electronic Voting Scheme Based on Revised-SVRM and Confirmation Numbers	2019	IEEE	Electronic voting, Revised-SVRM, ElGamal, RSA, Confirmation numbers, Anonymous credential	Revised-SVRM and Confirmation Numbers virtualization	To consider privacy, robustness, accuracy, integrity, incoercibility and fairness

METHODOLOGY

The development of model solutions/systems to the identified problems is essential to find appropriate research methods. This work applies the Systems Creation Life Cycle (SDLC) approach to obtain a stable electronic voting system that solves real-life problems. SDLC is the process of creating or modifying systems in systems engineering, information systems, and software engineering and the models and methods that people use to develop these systems. SDLC, in particular, the information system, is a method for design and implementation.

A clever iterative model is employed in this work. SDCL agile model is a method that ensures agility, flexibility and adaptability during the development and maintenance of software.

Requirements definition

Before designing any voting system, a comprehensive and detailed set of requirements have to be developed. The design requirements of the online voting system developed in this work are divided into two groups, namely, generic and system-specific. General requirements are requirements that apply to any voting system. The essential requirements of a system, on the other hand, are those that are specific to a developed system. System-specific requirements, on the other hand, are requirements that are specific to the developed system. Allows system-specific requirements of the system:

1. **Multi-user:** Several voters can vote simultaneously;
2. **Accessibility:** System access can be accessed by voters in any location using secure internet and mobile devices.

A framework design for the system

The framework design was done to determine applications architectural framework. The emerging framework from this design process represents the structure for the realization of the defined goal. An integral part of the model design is the infrastructural model architecting in which model(s) were developed on the framework. The models are graphical developed using unified modelling language (UML).

Software development

The software was developed and deployed to test the framework developed. The software was produced using HTML 5, PHP v6, MySQL server 2012, HTTP SMS gateway. Windows XP, Windows10 etc.

Performance testing and evaluation

Users understanding of the developed system were collected after experimental usage to ascertain if the core values desired in the voting system are inherent in the developed online voting system. The following research questions arose in the

guided bothering on whether the developed online voting system meets the desired general security requirements in voting systems:

1. Can a vote be without a reservation? The Requirement for “Integrity”.
2. Can a valid vote be included in the final tally? Requirement for “Accuracy”.
3. Can voters be verified as to who they claimed to be? Requirement for "Authenticity".
4. Can the developed online voting system only allow eligible voters to vote and only vote only once? Requirement for “Democracy”.
5. Can the developed online voting system ensure that no polling can be linked to the electorate or other voters? Requirement for "Privacy".

System Design

The system has three modules such as admin module, the client module and the server module. The admin module has functions like add/manage user, add/manage candidate, add/manage parties and view votes. The admin can add, update, and delete information related to the users, candidates and parties through this module. The client module includes an android application installed in the user's smartphone. The application requires users to register themselves and sign up using the same username and password when registering. The user then has to select the candidate he wants to vote for. Once the user clicks on the "Vote" buttons, his share 1 is sent to him by his email id, while share 2 is automatically uploaded through the server. Certified users will be shown a captcha that users must use properly. Correctly entered into the captcha, the user's vote will be successfully registered.

The System Architecture

For phishing detection and prevention, we are proposing a new method for detecting phishing websites. Our method uses visual cryptography, and it is based on an Anti-Phishing Image Captcha authentication scheme. It prevents passwords and other unique information from phishing websites. The proposed system can be divided into two phases one is the Registration phase, and the second is the Login phase.

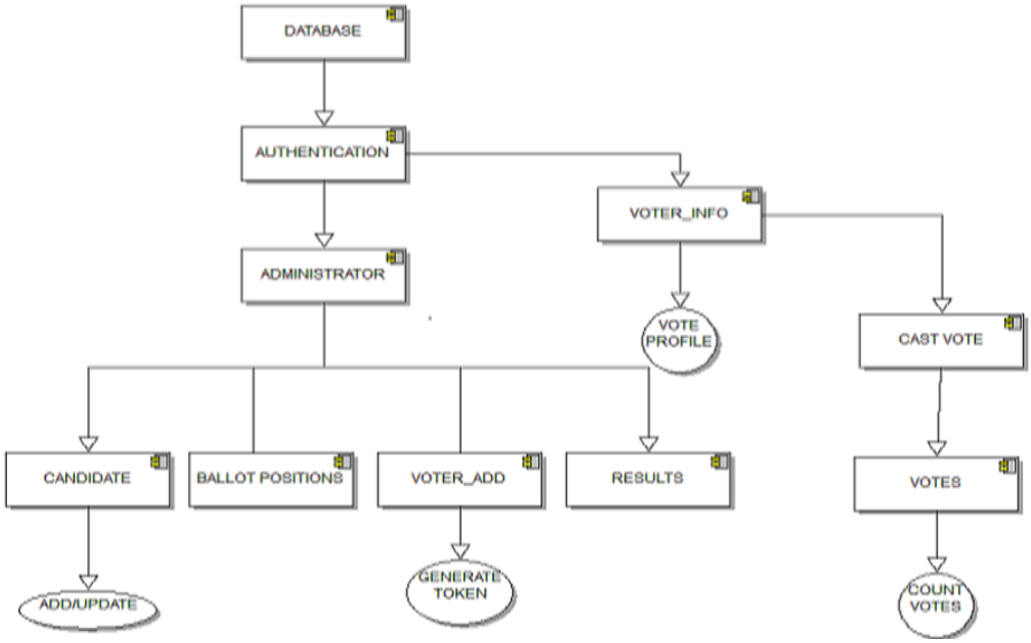

Fig 1 System Architecture

Registration Phase

During the registration phase, the server will select textual images as passwords. The text of these images will serve as the password for the user. The image is divided into two shares, one shared with the user and the other shared with the server. The user's share is sent to the user for further verification during the login phase. The image is also stored for the actual database of the website as confidential data.

Login Phase

In the Login phase, first, the user is asked for a username (user id) before a username. Then the users asked to enter their share, which is kept with them. This share is sent to the server where the user's share, which is stored in the website dataset for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user. The end users are required to enter the text displayed for image captcha, which can serve the purpose of password and using this, the user can log in to the website. Now, the user id and password will be sent to the authentication system for authentication. Authentication is the process of ensuring that the person is what she claims to be. For this purpose, the user id is sent to the server, and the corresponding password is fetched from the database. Now the password provided by the user and the password fetched from the database is compared. Therefore, using the username and image captcha generated by stacking two shares, one can verify whether the website is a real/secure website or a phishing website and check if the user is authenticated.

Datasets

The online voting system uses a database called **Online Voting consisting of two datasets as follows:**

1. **Registration details** - The table contains records of registered users/voters with relevant usernames and passwords. It also has voters/ user contacts, phone numbers, and email addresses.
2. **Vote details -** It contains the record of the candidate and the voters who voted in favour of the candidate. Its primary key is the id field which is also required during the vote count. The database is queried to find out how many voters' casts their votes for a given opponent.

CONCLUSION

Online voting using visual cryptography overcomes the limitations of the traditional voting system. This system provides more security, take some time. As well as there is no possibility of voter fraud, and the money spent on security could be drastically reduced. The main purpose of this method is to provide complete privacy to the voter and ensure optimal coordination of the online voting system. The basic idea of this system is to use a robust security mechanism for voter authentication. Visual cryptography encrypts information, and decryption can be performed without any use of mathematical calculations. People who have an internet connection at home can vote without any difficulty in the voting polls. Elections can be conducted relatively easily and effectively using this internet-based voting system using visual cryptography. The voter can vote from the place where he works using an online voting system. Internet-based voting offers many benefits, including low cost and voter participation. This voting system carefully considers security and human factors and, in

particular, ensures that they provide voters with reliable and intuitive indications of the validity of the voting process. The system we proposed uses visual cryptography to provide mutual authentication for voters and election servers.

REFERENCES

1. Ollmann G. The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.
2. M. Naor and A. Shamir (1994), Visual cryptography, in Proc. Eurocrypt, pp. 1–12.
3. A. Shamir (1979), .How to Share a Secret, Communication ACM, vol. 22, pp. 612-613.
4. G. R. Blakley (1970), .Safeguarding Cryptographic Keys, Proceedings of AFIPS Conference, vol. 48, pp. 313- 317.
5. A. Menezes, P. Van Oorschot and S. Vanstone (1997), .Handbook of Applied Cryptography, CRC Press, Boca Raton, FL, 1997.
6. Anderson C. (2006). How to Rig a Democracy: A Timeline of Electronic Voting in the United States. The Independent. Retrieved November 28, 2006, from: http://www.indypendent.org/?p=608
7. Bellis, M. (2007). The History of Voting Machines. Retrieved November 9, 2006, from:http://inventors.about.com/library/weekly/aa111300b.htm
8. Cranor, L.F., & Cytron, R.K. (1996).Design and Implementation of a Security-Conscious Electronic Polling System. Washington University Computer Science Technical Report (WUCS). Retrieved October 9, 2006, from: http://www.acm.org/crossroads/ords2-4/voting.html
9. Electronic Voting and Counting – Development of the System. (2005). Elections ACT. Retrieved February 11, 2007, from: http://www.elections.act.gov.au/EVACS.htmlhttp://www.iiec.or.ke/
10. Sumit Jagtap, Smitesh Vichare, Alpa Vaidya, Mangesh Jogd and Prof. Shivani Sthapak, "VC Technology in Internet Voting System", published in 4, April 2016.
11. Rajendra A B and Sheshadri H S," Visual Cryptography in Internet Voting System".
12. Pallavi V Chavan, Dr Mohammad Atique, and Dr Anjali R Mahajan, "An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", published in 2011.
13. Anusha MN and Srinivas B K," Remote Voting System for Corporate Companies using Visual Cryptography", published in 2012.
14. Sanjay Kumar, Manpreet Singh, "Design A Secure Electonic Voting System Using Fingerprint Technique", published in July 2013.
15. Olaniyi Olayemi Mikail, Folorunso Taliha Abiodun, Abdullahi Ibrahim Mohammed, Abdulsalam Kayode Abdusalam, "Design and Development of Secure Electronic Voting System Using Radio Frequency Identification and Enhanced Least Significant Bit Audio Steganographic Technique", published in Dec 2014.
16. Jena Catherine Bel.D, Savithra. K, Divya.M, "A Secure Approach for E-Voting Using Encryption and Digital Signature", published in 2015.
17. Badave Malhar S, Kadam Amit B, Nalawade Ranjit S, Hipparkar Abhijit A, "Review: Online Voting System Using Android", published in 3, March 2016.
18. William Robson Schwartz, Huimin Guo, Jonghyun Choi, Larry S. Davis, "Face Identification Using Large Feature Sets", published in 4, April 2012.
19. L. Rural al., "Analysis of Image Steganography Techniques in Secure Online Voting", in Proceedings of IEEE International

Conference on Computer Science and Network Technology (ICCSNT), pp.120–124, 2011. http://dx.doi.org/10.1109/ICCSNT.2011.6181922

20. L. Ruraet al., "Online Voting Verification with Cryptography and Stenography Approaches", in Proceedings of IEEE International Conference on Computer Science and Network Technology(ICCSNT), pp.125–129, 2011. http://dx.doi.org/10.1109/ICCSNT.2011.6181923