MANTECH Publications
Recent Trends in Computer Science and Software Technology
Volume 6 Issue 3, September-December 2021

A Study of Robust Cryptography to Ensure Safe Online Voting

Surbhi Vashisht, Gayatri Pandey
Assistant Professor[1], Student[2]
Department of CSE
Yeshwantrao Chavan College of Engineering (YCCE)
Corresponding Author's E-mail: *Pgayatricse@gmail.com*

Abstract

Few individuals vote these days because of their hectic lifestyles. There is a multitude of reasons for this, including the requirement for some to go to the polls, the need to wait in long lines, and the fact that many people are weary due to their hectic schedules. As a result, we created a voting system that is accessible over the internet. This strategy, however, has several drawbacks. Phishing attackers legally acquire client credentials and utilise the proper secret passwords to access critical websites. Consider a web-based voting system for corporate organisations, in which members vote once a year to elect a president, secretary, or key management. On election day, every voter must converge in one area to cast his or her ballot under the current system. We use a distinct approach termed visual cryptography in this strategy. In this design, we use visual data for security. In this step, we split the one-of-a-kind image into two halves, each of which is kept in a separate database. When these two are intertwined, we obtain the original picture. When we get our hands on the original image, we use it as a secret password. This method is incredibly handy and well-suited for online remote voting. Because this is an electronic application, it may be accessed via the web through any lawful personal space on the planet.

Keywords: *Online Validation, Online voting, Visual Cryptography, Phishing attack, Cyber security, Privacy, encrypted password*

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

INTRODUCTION

Elections are held throughout the country. Voters must, however, attend to the polling booth to vote. The political membership process is quite complicated, and numerous things are required to move the voting process forward. To conclude, extensive preparations have been done. It entails manual labour. Government elections are held on a district-by-district basis. To vote, the voter must be present at the polling station. This may lower voter support; yet, web-based voting streamlines the process. Voting in visual cryptography entails some level of security. It is critical to have such mechanisms in place. This will minimise labour, make ballet more accessible, and increase productivity. Individuals must be available for selection at the place. Visual cryptography is a method of encoding images. During registration, the customer will be contacted and asked to supply a security image. The security portion of the security photo will be emailed to the consumer. This file will be shared in encrypted mode. The customer can alter the details at any moment by logging into the system. The consumer is just required to upload a security share while voting. Because the security share is produced using random pixels, the true picture cannot be anticipated, hence the poll cannot be voted on if the share is inaccurate. Furthermore, because the information will be securely delivered by email, it cannot be recovered by any other client or unapproved person. Ballet casting will be productive only if the right share for that customer is uploaded.

Fraud delivers bogus communications or puts up bogus websites that mimic the real thing. Phishing is a type of online identity theft in which fraudsters deceive Internet users into giving personal information to fraudulent websites. Phishing scams are typically disguised as spam or pop-ups and are notoriously difficult to detect. When fraudsters gain your personal information, they might use it to commit various types of identity theft, jeopardising your good name and reputation. Fishers' bogus sites will get increasingly advanced in design. Phishing is one of the sorts of fraud, therefore you should be familiar with a range of phishing methods as well as find out how to prepare for it. The simplest and most straightforward approach to safeguard a system asset is to give it a unique name and a password.

The study of data encryption is known as cryptography. It has been utilised as a secure way of communication between individuals and governmental agencies.

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

Today, cryptography serves as the foundation for advanced security solutions that are used to protect data and assets on both open and closed networks. Belief is the process of assessing a person's or thing's characteristics. The objective of confirming anything is to ensure that you have a genuine agreement. The goal of confirming a person is to ensure that you are not operating an imposter. It is important to develop their own techniques in order to identify the degree of permission of the application's user. Applications frequently do this by retaining private records that include the names of consumers and who has access to them. Database applications, for example, create private approval tables on a regular basis to regulate which fields in a record a given client can read or alter. There are several sorts of Internet-based apps. The web-based voting method is one of them. Few individuals advocate for the benefits it delivers, such as mobility, openness, and enhanced speed and accuracy in the delivery of ballots from home, while the same number is concerned about the problems, such as inconsistent entry, breach of mystery, and ambiguity. As well as a shift in the impact of political race. The project employs visual cryptography to avoid phishing attempts and ensure the authentication of Internet voting systems. Visual cryptography is a type of encryption scheme that uses images to disguise data so that it may be deciphered by human eye if the correct key picture is used.

SURVEY OF THE LITERATURE

From the beginning of time to the present day, there have been online voting methods. This study has clarified those points. Create voting plans that will allow you to employ ICT resources to deliver more efficient voting services than traditional paper-based voting techniques. Voters consider themselves customers, and the government is supposed to make voting more convenient. Various forms of electronic voting, in particular, have attracted considerable attention over the last decade 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 different types of Internet or remote electronic voting systems are being used with varied degrees of effectiveness. Although some systems were doing successfully, some were abandoned, and others were implemented owing to security concerns.

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

There are three different types of voting systems:

1) System of paper ballots

The most extensively used standard voting technology is the paper ballot mechanism. It will be utilised before the electronic voting system is implemented. The paper ballet method is made up of two parts: paper ballet and sealed ballet. Every voter uses a single ballot and does not share it. The disadvantages of this approach are: I it is time intensive; and (ii) it has a slow telly speed.

2) Electronic voting machine

A voting system that employs electronic ballots to allow voters to communicate their secret ballots to election authorities over the Internet is known as an electronic voting system. This method has the following drawbacks: I persons with limited computer expertise cannot vote effectively; (ii) it is vulnerable to security risks; (iii) polling station power consumption; and (iv) prices.

3) System of online voting

The most recent electronic voting technology is the online voting system, in which the ballot is transmitted over the Internet using a web browser. Voters from all around the globe can vote online. The sole disadvantage of utilising this programme is the lack of security.

There are various security concerns with internet voting:

Most applications provide strong password protection and do not target phishing attempts. Attackers gain users' credentials directly through phishing, and with the proper password, they may access the necessary web pages. There is no effective method for protecting website visitors from phishing.

To address the security criteria for online voting privacy, secrecy, eligibility, fairness, verification, and receipt, a secure Internet-based online voting system was developed utilising an identity-based encryption technology.

The major suggested blind more secure online voting protocol to fulfil the security criteria of privacy, anonymity, eligibility, fairness, verification, and the uniqueness of safe online voting.

Two millionaire couples invented an identity-based safe online voting system based on cryptographic algorithms that meet the requirements of privacy, eligibility, transparency, accuracy, and uniqueness for secure e-voting.

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

Table of Comparisons

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-voting system.	Functional digital signature foranonymously issuing a blank ballot to a voter and used the BLS short signature scheme for protecting the vote from any modification.	The future of voting: End-to-end verifiable internet voting-specification and feasibility study
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, multi-threading, 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 technique at an input unit
3	Avoiding Phishing Attack on Online Voting System Using Visual Cryptography	2020	Springer	Visual Cryptography; CAPTCHAImage	Visual Cryptography Technique used to detectt phishing site or original site easily.	we will be designingan efficient voting system for Carrom Association that will prevent phishing attack.
4	Secure Electronic Voting Using a Hybrid	2019	Science direct	SDLCmethodfor design and implementation of voters	hybrid cryptosystem and steganography	The direction of future works can be tuned

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

	Cryptosystem and Steganography			information system. This work employed the iterative waterfall model.	was developed, attempt to proffer a more robust scheme in fulfilling the security requirements for electronic voting.	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 Block chain for Secured Voting Scheme	2019	IEEE	Block chain, 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 by fingerprint or face recognition inreal time implementation.
6	SeVEP: Secure and Verifiable Electronic Polling System	2019	IEEE	Authentication, efficiency, electronic polling, malware, security, verifiability.	Resource allocation pollingsystem haveAuthentication, process of electronic polling.	develop a working prototype of SeVEP, and evaluate its scalability and usability in real-world deployment.
7	Towards Developing a Secure and Robust Solution for E-Voting using Block chain	2019	Springer	coercion resistance problem, Blockchain, Online Voting process	Developing a SecureSolution for online Eelection process information	To solve coercion resistance problem to solve, cryptographic algorithms

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

8	E2E Verifiable Electronic Voting System for Shareholders	2019	IEEE	Electronic voting, Shareholder voting, End-to-end verifiability, Zero knowledge proofs, Decisional Diffifie Hellman assumption, Security proof.	Verifiable election process	More general case that voters to use a smart phone may depart and leave dynamically within 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 Numbersvirtualization	To consider privacy, robustness, accuracy, integrity, incoercibility and fairness

METHODOLOGY

It is critical to construct model solutions / systems to the highlighted challenges in order to locate relevant research methodologies. This study use the Systems Creation Life Cycle (SDLC) technique to create a robust electronic voting system that solves real-world concerns. SDLC refers to the process of developing or updating systems in systems engineering, information systems, and software engineering, as well as the models and methods used to do so. SDLC, in particular the information system, is a design and implementation process. This work employs a sophisticated iterative model. The SDCL agile model is a way for ensuring agility, flexibility, and adaptation during software development and maintenance.

Definition of requirements

A complete and clear set of requirements must be defined prior to constructing any voting system. The design criteria for the online voting system created in this study are classified as general and system-specific. The general requirements are those that apply to every voting system. A system's essential needs, on the other hand, are those that are unique to a created system. System-specific needs, on the

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

other hand, are those that are unique to the created system. Allows for system-specific system requirements:

i. Multi-user: Multiple voters can vote at the same time; ii. Accessibility: Voters can access the system from any location by utilising secure internet and/or mobile devices.

Design of the System Framework

The framework design was completed in order to identify the architectural structure of the apps. The framework that emerges from this design process is a representation of the structure for achieving the desired goal. The infrastructural model architecting, in which model(s) were constructed on the framework, is an essential aspect of the model design. The models are graphical models created using the unified modelling language (UML).

To test the framework, software was created and deployed. HTML 5, PHP v6, MySQL server 2012, and HTTP SMS gateway were used to create the app. Windows XP, Windows 10, and so on.

Evaluation and testing of performance

Following trial use, users' perceptions of the produced system were gathered to determine if the basic qualities required in a voting system are inherent in the established online voting system. In the guided investigation into whether the constructed online voting system fits the intended general security criteria in voting systems, the following research concerns arose:

1. Is it possible to vote without a reservation? The "Integrity" Requirement
2. Is it possible to include a legitimate vote in the final tally? "Accuracy" is a requirement.
3. Can voters be confirmed to be who they claim to be? "Authenticity" is a must.
4. Will the planned online voting system only enable eligible voters to vote once? "Democracy" is a prerequisite.
5. Is the created online voting system capable of ensuring that no polling is linked to the electorate or any other voter?
   "Privacy" is a must.

Design of a System

The system is divided into three modules: admin, client, and server. The admin module includes operations such as adding/managing users, adding/managing candidates, adding/managing parties, and viewing votes. Through this module, the administrator may add, amend, and delete information about users, candidates, and

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

parties. The client module consists of an Android application that is installed on the user's smartphone. The programme asks the user to register and then sign up using the same username and password that they used to register. The user must next pick the candidate for whom he or she wishes to vote. When a user hits the "Vote" buttons, share 1 is delivered to his e-mail address, while share 2 is instantly uploaded through the server. Certified users will be shown a captchat that must be used correctly. The user's vote will be successfully registered if the captcha is correctly typed.

The Architecture of the System

We propose a novel approach for recognising phishing websites for phishing detection and prevention. Our technique is based on an Anti-Phishing Image Captcha authentication mechanism that employs visual cryptography. It protects passwords and other personal information from fraudulent websites. The suggested system is broken into two phases: the registration phase and the login phase.

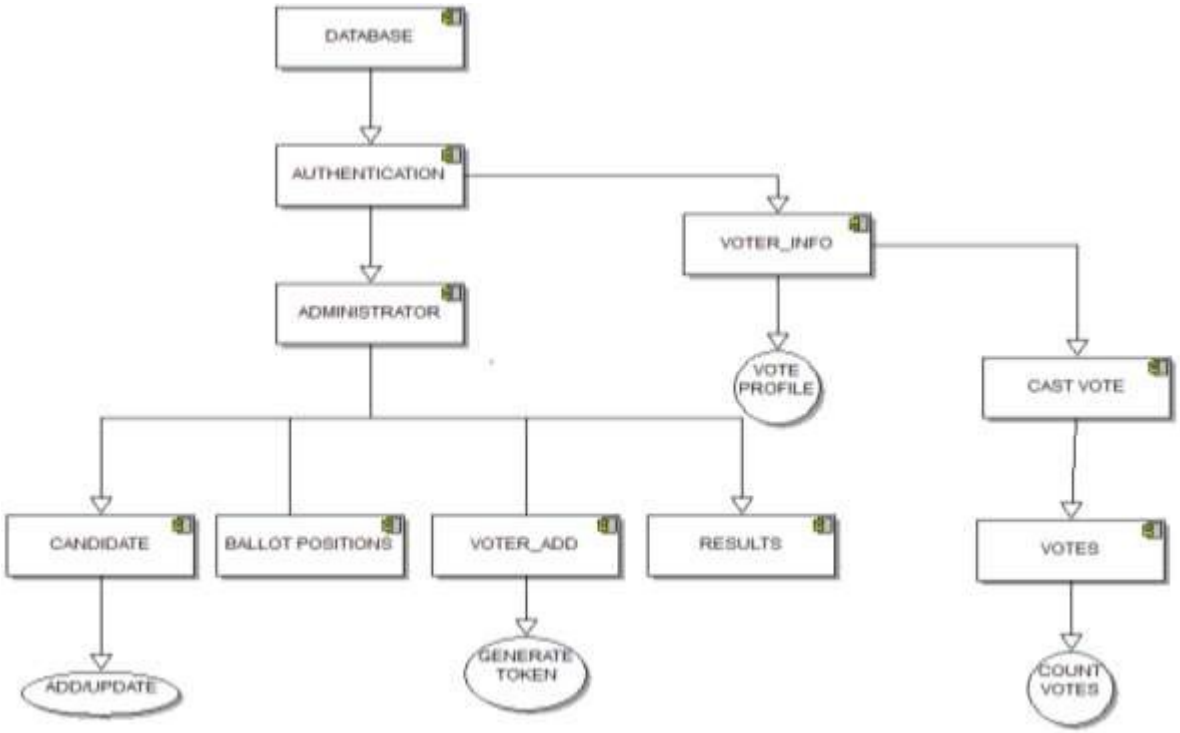


Figure 1 depicts the system architecture.

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

Phase of Registration

The server will choose textual pictures as passwords during the registration step. The text in these photos will be used as the user's password. The picture is separated into two shares, one with the user and one with the server. During the login step, the user's share is provided to the user for additional verification. The photograph is also saved in the website's database as sensitive data.

Phase of Login

During the Login phase, the user is initially requested for a username (user id) before a password.

The users were then requested to enter his share, which he retained. This share is sent to the server, where the user's share and the share stored in the website's dataset for each user are stacked together to generate the picture captcha. The user is presented with a picture captcha. The end user is needed to type the text presented for picture captcha, which might function as a password and allow the user to log in to the website. The user id and password will now be transmitted to the authentication system for authentication. The process of establishing that a person is who she claims to be is known as authentication. The user id is provided to the server for this reason, and the appropriate password is retrieved from the database. The password given by the user and the password retrieved from the database are now compared. As a result, given the username and picture captcha formed by stacking two shares, one can determine if the website is genuine/secure or a phishing website, as well as whether the user is authorised or not.

Datasets

The online voting system makes use of a database named Online Voting, which is made up of two datasets:

1. Registration information - The table contains records of registered users/voters together with their respective usernames and passwords. It also includes voter/user contact information, phone numbers, and email addresses.

2. Vote information - It covers the candidate's voting record as well as the voters who supported the candidate. The id field is its primary key, and it is also necessary during the vote count. The database is searched to determine how many voters voted for a specific opponent.

CONCLUSION

The use of visual cryptography in online voting overcomes the constraints of the

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

traditional voting mechanism. Take your time using this method because it gives additional security. Furthermore, there is no danger of voter fraud, and security costs might be greatly lowered. The fundamental goal of this strategy is to give total anonymity to the voter while also ensuring that the online voting system runs smoothly. The primary concept behind this approach is to employ a strong security method to authenticate voters. Visual cryptography encrypts data and allows for decryption without the use of mathematical computations. People who have an internet connection at home may easily vote in the voting booths. Elections may be held reasonably simply and successfully utilising this internet-based voting method based on visual cryptography, as the voter can vote from his workplace using the online voting system. There are several advantages to using the internet to vote, including lower costs and more voter turnout. This voting system carefully examines security and human issues, ensuring that voters get accurate and intuitive signs of the voting process's legitimacy. We presented a method that uses visual cryptography to offer mutual authentication for voters and election servers.

REFERENCES

1. Ollmann G. The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software InsightSecurity 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 theUnited 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

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

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. SumitJagtap, SmiteshVichare, AlpaVaidya, MangeshJogd and, Prof. ShivaniSthapak, "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, HuiminGuo, Jonghyun Choi, Larry S. Davis, " Face Identification Using Large Feature Sets", published in 4, April 2012.
19. L. Ruraet al., "Analysis of Image Steganography Techniques in

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved

Secure Online Voting", in Proceedingsof IEEE International Conference onComputer Science and Network Technology (ICCSNT), pp.120–124, 2011. http://dx.doi.org/10.1109/ICCSNT.2011.6181922

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

Page 83-95 © MANTECH PUBLIATIONS 2021. All Rights Reserved