International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 12 | Dec 2024 www.irjet.net p-ISSN: 2395-0072

The Development of a Secure Online Web-Based Voting System for Corporate Elections

Bindushree A N[1],Lavanya N G[2], Basava H K[3], Harsha S Kulambi[4]

[1]*Bachelor of Engineering, Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, affiliated to VTU Belagavi, Karnataka, India.*
[2]*Bachelor of Engineering, Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, affiliated to VTU Belagavi, Karnataka, India.*
[3]*Bachelor of Engineering, Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, affiliated to VTU Belagavi, Karnataka, India.*
[4]*Bachelor of Engineering, Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, affiliated to VTU Belagavi, Karnataka, India.*

Abstract - In addition to requiring significant social and human resources, the voting process in a traditional voting environment can occasionally become highly inconvenient since some voters are reluctant to go to a polling place to cast their ballots. Internet voting is made easier by the advancement of computer networks and the development of cryptography mechanisms. We present a secure internet in this paper. voting procedure that can be used for online voting. The suggested voting mechanism will work for big companies with offices spread across multiple locations and is based on digital signatures and cryptography. Three separate phases make up the suggested system: the registration phase, the authentication phase, the voting phase, and the counting phase, which involves the voter, voting server, and voting authority

Key Words: Internet voting, digital signatures, and web servers

1.INTRODUCTION

In today's democratic world, the phrases election and voting are now widely used. Internet-based electronic voting would be far more lucrative. Many voters would value the ability to cast a ballot from any location. Employees from every office can participate in the election from their own offices if the company has offices spread across multiple regions and uses online voting. As the name suggests, electronic voting is a voting procedure conducted by computers or other electronic media. Generally speaking, an online voting system should meet the following criteria:

1. Accuracy
2. Simplicity
3. Democracy
4. Verifiability
5. Privacy
6. Security

Security and privacy are the primary concerns for such an online voting system, and from that perspective, implementing a secure Internet voting system seems to be another application of cryptography and network security. Electronic voting has been extensively researched over the past 20 years, and numerous e-voting systems have been proposed in the last few decades, increasing both security and effectiveness. However, to the best of our knowledge, no comprehensive and workable solution has been found for large-scale elections conducted over a network, such as the Internet.

Our method proposes a useful implementation of current cryptographic techniques and digital signatures that guarantee voter authentication and the integrity of the vote cast. on both levels. Since every voting system criterion must be satisfied, designing a secure electronic voting system over a network is in fact an extremely challenging process. If even one of the standards is not followed, there may be flaws and kinks that a third party could use to alter or fabricate the finer points. The election's outcome is then determined by adding up all of the votes, which the authorities jointly decipher. Voters must be able to keep their votes secret under a voting system

2. Literature Survey

This study [1] reviews the vote verification techniques that are currently in use. By talking about their shortcomings, we can suggest a stronger and more dependable vote verification system. approach. The authors of this study aimed to suggest a vote verification method that would allow all election participants to verify votes and be able to verify votes against significant potential threats. They must look at a mix of procedural and technical options to achieve this goal. They must look into a combination of technological and procedural solutions for this reason.

The design for electronic voting systems based on trustworthy web services was suggested by the author [2].

The findings from the examination of the suggested design's evaluation showed that solution, significantly improve the dependability. outlined how this architecture can address the primary needs of electronic voting. One of the most crucial characteristics and the most crucial prerequisite for electronic voting, along with security, is availability, which is met. Since security is a crucial component of electronic voting systems, the author has employed pre-existing techniques to accomplish web service security. The author of the study [3] suggested an architecture for an online voting system that relies on trustworthy web services. He then used Reward Petri Nets and RBD to model this system. Lastly, he conducted a quantitative evaluation of these models. He can choose whether or not to apply this system by also considering the evaluation's findings. It is evident that his architecture significantly improved reliability. He also took into account the primary criteria for voting, such as confidentiality, portability, precision, originality, and so forth. He employed a few strategies to develop a secure system while keeping in mind the security requirements of voting. He demonstrated that even if some parts fail, this system will still function, and that availability and security are the The most crucial voting system specifications will be covered. Voters can vote online with ease and without spending any time or money. Thus, systems have the ability to motivate people to vote.

The author [4] suggested an electronic voting process that guarantees the accuracy and anonymity of voters and candidates. There are still a lot of problems, as when a lot of voters Will there be a denial of service (DOS) on the Internet if they cast their votes simultaneously? How can a safe and effective online voting system be created? However, the several measurement levels included in our plan have reduced the possibility of injustice in real elections, at least for the counting process

According to the suggested design in paper [5], voting is only permitted at the locations where voting stations are set up. Despite the fact that mobile terminals can be used for voting Depending on the wireless conditions, extra security standards will be needed everywhere if the wireless network continues to grow in the days ahead. Additionally, the authentication process needs to be strengthened, and there shouldn't be any forced voting or data disclosure on the wireless network. One important method that democracy reflects the will of the country is by voting. For this reason, further research on security technologies used with electronic voting systems should be ongoing.

An online voting procedure was presented by the author [6]. Blind signatures are used in the proposed internet voting protocol to safeguard ballot content while it is being cast. As we feel that a secure electronic voting system prevents ballot buying and enables all voters to confirm the outcome of the vote. The suggested internet voting protocol is both verifiable and deters ballot purchasing. During the election, any unapproved party or candidate may still attempt to purchase ballots. However, once the election results are announced, no voter can demonstrate whose ballot they cast. To put it another way, ballot purchasing may still occur, but the buyer cannot be certain that the voter will mark the ballot in the way that they desire.

3. Participants and Phases

Voters, voting clients, voting servers, and voting authorities are the participants. The following phases will make up the system:

1.Enrollment
2.Verification
3. Casting a ballot
4. Counting

Phase of registration: An authorized representative of the corporation will visit each office and, after confirming an employee's identity, register them to vote and Give him or her the username and password. For security reasons, the voter can subsequently change their password online, just like they can when they first receive their ATM card and PIN from the bank.

Phase of voting: During this stage, the first ballet request is made. The public encryption key and ballet will be sent to the voter. This key will be used to encrypt the vote. That encrypted vote is once more utilize the voter private key to digitally sign. The voting server receives the digital signature and encrypted vote. The voting server stores the encrypted vote after first verifying the digital signature.

Phase of counting: All encrypted votes are first decoded before being counted. To decrypt, the authorized individual will input the private decryption key. The After counting is complete, the outcome will be announced.

4. System Architecture

This system is being designed for a company with offices spread throughout several cities. Our top priority is to ensure the security of the cast ballot while it is being transported from We are concentrating on offering security against both passive and active intruders when it comes to voter to voting server storage. A voter's cast ballot can be accessed by a passive invader, posing a threat to the voting system's privacy and confidentiality features. The active invader may interfere with the integrity of the cast vote and tamper with it. Therefore, we are utilizing the idea of cryptography and utilizing digital signatures to address this security issue. In order to protect against passive intruders, we are encrypting the client system's cast vote before sending it to voting server via the internet, where the vote is decrypted on the server side prior to counting. For this, we need two keys: one for the voter system's encryption, which

should be known to the public, and another for the decryption of the encrypted vote prior to its counting on the voting server, which needs to be private. Therefore, two asymmetric keys are required for this purpose.

We are utilizing digital signatures to protect against active intruders who could change or tamper with the cast vote while it is moving from voter to voting server. When a voter After casting his or her ballot, the voter will digitally sign it using their own private digital signature and send it to the voting server, where the voter's publicly known digital signature verifier will verify the signature. We are using a pair of asymmetric keys for every registered voter in order to achieve this goal, which calls for each voter to have a private digital signature and a public digital signature verification. As shown in picture 1

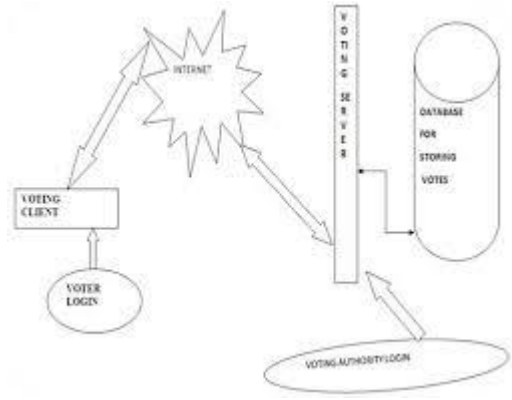

Figure1: Web-based online voting system design comprise the voting authority, voting client, voting server, and voter. A voter who has registered connects to the voting server by utilizing his password and access credentials. Through the internet, the voting client and voting server exchange information.

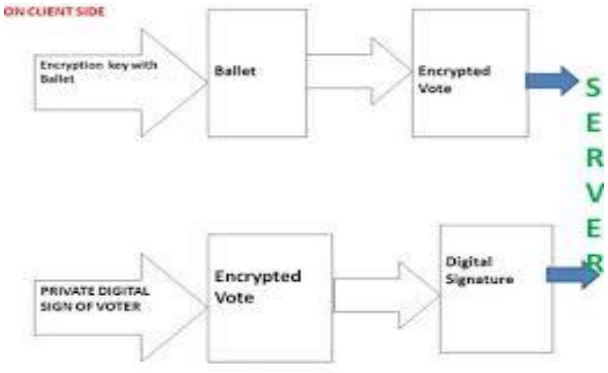

Figure 2: Client-side computing for voting

When a voter wants to cast a ballot, he first requests a ballet from the server, which then sends the ballet together with the public encryption key, as shown in figure 2. The voter encrypts cast a ballot with this key, and then used his private key to digitally sign the encrypted ballot. and forward them both to the server. Using a public signature verifier, the voting server uses decryption to validate the voter's digital signature on the server side. Voting is stored if the signature is legitimate. for counting; if not, the vote is eliminated.

5. Results and Implementation

In order to register voters, the authorized voting authority will visit each company's office and manually confirm each employee's identity. When registering to vote create a pair of asymmetric keys, one private and one public. The voter keeps his private key private, and the public key is sent to the server along with his other voter registration information.

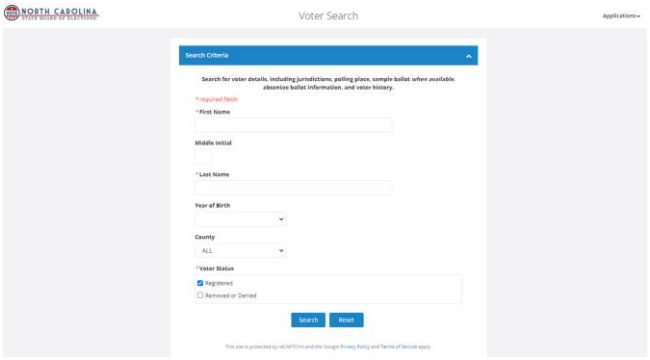

Figure 3: Voter registration form on a screen

Voters can modify their password for security reasons by logging in to the website.

Figure 4: Voter Registration Form

Voters log in with their own username and password on election day. The server sends the ballet together with the public encryption key when the voter requests it. The voter voted and uses a public encryption key to encrypt it.

Figure 5: a vote-casting image of Ballet

Every candidate running for office has an ID that we have internally allocated, and when a voter casts his or her ballot, the ID is encrypted using a public encryption key that Ballet provides. The voter then uses their own private digital signature to digitally sign that vote. And forward these two to the server.

Figure 6: shows a picture of Ballet following digital signature and encryption.

The vote is encrypted, so if a passive intruder manages to access the cast vote, he cannot determine who the voter is. If an active hacker changed the vote and sent it to the polls Because the vote is digitally signed, the server can easily detect when a vote has been edited. When the server verifies the signature, it discovers that the vote has been altered and notifies the voter of this.

6. Conclusion

After conducting tests on our system, we have determined that it offers protection against all kinds of attacks when the vote is moving from the voting client to server for voting. Security risks from both active and passive intruders are included in these attacks. This technique can also be used to get staff opinions on particular matters. In the future, voter authentication will be more secure if we can utilize the voter's thumb impression or take a picture of their face and compare it with a photo in our database rather than using their username. Compared to a regular voting system, this one saves money and time. It also prevents paper waste and is environmentally beneficial.

References

[1] "Vote Verification through Open Standard: A Roadmap," by Ali Fawzi Najm Al-Shammari and Sergio Tessaris, 978-1,4577- 0953-1/11IEEE2011.

[2] "An Architecture for E-Voting Systems Based on Dependable Web Services," by Amir Omidi and Mohammad Abdollahi Azgomi IEEE©2009978-1-4244-5700-7/10

[3] Saeed Moradi and Amir Omidi, "Quantitative Assessment and Modeling of an Internet Voting System Using Dependable 978-1- 4673-0479-5/12/©2012 IEEE

[4] Web Services

[5] Haijun Pan, Edwin Hou, and Nirwan Ansari, "Protecting the Privacy of Voters and Candidates in Electronic Voting Systems" IEEE ©2011 978-1-61284-680-4/11/$26.00

[6] An analysis of the electronic voting system employing blind signatures for anonymity was presented by Seo-Il Kang and Im Yeong Lee at the IEEE 2006 International Conference on Hybrid Information Technology (ICHIT'06) 0-7695-2674-8/06.

[7] "A Verifiable Electronic Voting Scheme," Chun-Ta Li, Min-Shiang Hwang, and Yan-Chi Lai, 2009 Sixth International Conference on Information Technology: New Generations

[8] "Distributed eVoting using the Smart Card Web Server" by Lazaros Kyrillidis, Sheila Cobourne, Keith Mayes, Song Dongy, and Konstantinos Markantonakis 3/12/2012 978-1-4673-3089 IEEE

[9] "Watermarking in e-voting for large scale elections," by Yousfi Souheib and Derrode Stephane, 978-1-4673-1520-3/12/$31.00 ©2012 IEEE