IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 2, November 2023

I-Voting System

Prof. Harish Chandra Maurya[1], Harsh Kushwaha[2], Akhil Malap[3], Shubham Shinde[4], Ashish Kharat[5]

Assistant Professor, Department of Computer Engineering[1]
Student, Department of Computer Engineering[2,3,4,5]
Chhatrapati Shivaji Maharaj Institute of Technology, Panvel, Maharashtra, India

Abstract*:* *Online voting is a trend that is gaining momentum in modern society. It has great potential to decrease organizational costs and increase voter turnout. It eliminates the need to print ballot papers or open polling stations—voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they introduce new threats. A single vulnerability can lead to large-scale manipulations of votes. Electronic voting systems must be legitimate, accurate, safe, and convenient when used for elections. Nonetheless, adoption may be limited by potential problems associated with electronic voting sys- tems. Blockchain technology came into the ground to overcome these issues and offers decentralized nodes for electronic voting and is used to produce electronic voting systems mainly because of their end-to-end verification advantages. This technology is a beautiful replacement for traditional electronic voting solutions with distributed, non-repudiation, and security protection characteristics. The following article gives an overview of electronic voting systems based on blockchain technology. The main goal of this analysis was to examine the current status of blockchain-based voting research and online voting systems and any related difficulties to predict future developments. This study provides a conceptual description of the intended blockchain-based electronic voting application and an introduction to the fundamental structure and characteristics of the blockchain in connection to electronic voting. As a consequence of this study, it was discovered that blockchain systems may help solve some of the issues that now plague election systems. On the other hand, the most often mentioned issues in blockchain applications are privacy protection and transaction speed. For a sustainable blockchain-based electronic voting system, the security of remote participation must be viable, and for scalability, transaction speed must be addressed. Due to these concerns, it was determined that the existing frameworks need to be improved to be utilized in voting systems.*

Keywords: Blockchain-based electronic voting, Coding, Security, privacy

I. INTRODUCTION

I-voting or online voting is a system of voting where people can vote directly from their mobile, anytime and from anywhere. It is a revolution which is disrupting the traditional election systems with the power of the internet. In I-voting, voter can confirm if his/her vote has gone to correct candidate/party are major concern. I-voting could also reduce the number of errors made by both the voters and the electoral administrators.

Electoral integrity is essential not just for democratic nations but also for state voter's trust and liability. Political voting methods are crucial in this respect. From a government standpoint, electronic voting technologies can boost voter participation and confidence and rekindle interest in the voting system. As an effective means of making democratic decisions, elections have long been a social concern. As the number of votes cast in real life increases, citizens are becoming more aware of the significance of the electoral system. The voting system is the method through which judges judge who will represent in political and corporate governance. Democracy is a system of voters to elect representatives by voting. The efficacy of such a procedure is determined mainly by the level of faith that people have in the election process. The creation of legislative institutions to represent the desire of the people is a well-known tendency. Such political bodies differ from student unions to constituencies. Over the years, the vote has become the primary resource to express the will of the citizens by selecting from the choices they made.

The traditional or paper-based polling method served to increase people's confidence in the selection by majority voting. It has helped make the democratic process and the elec- toral system worthwhile for electing constituencies and governments more democratized. There are 167 nations with democracy in 2018, out of approximately 200, which are either wholly flawed or hybrid . The secret voting model has been used to enhance trust in democratic systems since the beginning of the voting system.It is essential to ensure that assurance in voting does not diminish. A recent study revealed that the traditional voting process was not wholly hygienic, posing several ques- tions, including fairness, equality, and people's will, was not adequately quantified and understood in the form of government.

Engineers across the globe have created new voting techniques that offer some anti- corruption protection while still ensuring that the voting process should be correct. Technol- ogy introduced the new electronic voting techniques and methods, which are essential and have posed significant challenges to the democratic system. Electronic voting increases election reliability when compared to manual polling. In contrast to the conventional voting method, it has enhanced both the efficiency and the integrity of the process . Because of its flexibility, simplicity of use, and cheap cost compared to general elections, electronic voting is widely utilized in various decisions. Despite this, existing electronic voting methods run the danger of over- authority and manipulated details, limiting funda- mental fairness, privacy, secrecy, anonymity, and transparency in the voting process. Most procedures are now centralized, licensed by the critical authority, controlled, measured, and monitored in an electronic voting system, which is a problem for a transparent voting process in and of itself.

On the other hand, the electronic voting protocols have a single controller that oversees the whole voting process. This technique leads to erroneous selections due to the central authority's dishonesty (election commission), which is difficult to rectify using existing methods. The decentralized network may be used as a modern electronic voting technique to circumvent the central authority.

Blockchain technology offers a decentralized node for online voting or electronic voting. Recently distributed ledger technologies such blockchain were used to produce electronic voting systems mainly because of their end-to-end verification advantages. Blockchain is an appealing alternative to conventional electronic voting systems with features such as decentralization, non-repudiation, and security protection. It is used to hold both boardroom and public voting. A blockchain, initially a chain of blocks, is a growing list of blocks combined with cryptographic connections. Each block contains a hash, timestamp, and transaction data from the previous block. The blockchain was created to be data-resistant. Voting is a new phase of blockchain technology; in this area, the researchers are trying to leverage benefits such as transparency, secrecy, and non- repudiation that are essential for voting applications. With the usage of blockchain for electronic voting applications, efforts such as utilizing blockchain technology to secure and rectify elections have recently received much attention.

II. PROBLEM STATEMENT

The main problem was related to trusting the EVM through i-voting we can make the process transparent for the voters and more easier. Offline voting was time consuming and sometimes irritating due to long queues which reduced the voters % , online voting will be less time consuming and comfortable from our convenient place which will increase the voting turnout %.In current voting system there are chances of false voting, duplicate voting , pressurized votes we can overcome this by giving the voter multiple chances to vote and the last vote will be considered as the correct one.

Into the i-voting system, our whole process is depends on internet if a user faces lack of internet connection or disconnection their vote will be on hold until the internet connection restores

III. PROOPOSED SYSTEM ARCHITECTURE

Our Proposed system will detect viruses if device is virus free then only voters are allowed to vote It provides high- level security because of smart contract and RSA encryption algorithm. It's a Progressive Web App(PWA) means if there is no internet connection then also your vote will be counted. It will be accessible over the internet.

Existing system turnout voters from 1952 election till today is ranging from 50 to 65% but our proposed system can ranged it between 80% to 95%.Our Proposed system is easy to use therefore no human/insider required for guidance. There is no misuse of data mismanagement while the website development is under process

IV. METHODOLOGY

Carefull planning and security considerations are essential when desigining an internet voting (i-voting) system. Here is a jigh-level implementation strategy for such a system ;

- Feasibility Study: Determine whether I-voting is practical for your community or organization , taking into consideration logistical , technological , and legal factors.
- Legal and Regulatory: Franework-Assure that local, state , and federal election rules are – Specify the parameters for I-voting eligibility .
- Security Planning: Create a through security framework with techniques for encryption, authentication, and authorization,- to increase confidence, think about implemaeting end-to-end verified solutions.
- Voter Registration: Create a strong voter authentication procedure , perhaps utilizing multi-factor authentication . Securely confirm each voters identity.
- Voter Registrtation: Establish an internet system for registering voters. Check the veracity of the registration data and the voter eligibility.

V. PROBLEMS AND SOLUTIONS OF DEVELOPING I- - VOTING SYSTEM

Whether talking about traditional paper-based voting, voting via digital voting machines, or an online voting system, several conditions need to be satisfied:

- Eligibility: Only legitimate voters should be able to take part in voting;
- Unreusability: Each voter can vote only once;
- Privacy: No one except the voter can obtain information about the voter's choice;
- Fairness: No one can obtain intermediate voting results; Soundness: Invalid ballots should be detected and not taken into account during tallying;
- Completeness: All valid ballots should be tallied correctly.

Below is a brief overview of the solutions for satisfying these properties in online voting systems.

ELIGIBILITY

The solution to the issue of eligibility is rather apparent. To take part in online voting, voters need to identify themselves using a recognized identification system. The identifiers of all legitimate voters need to be added to the list of participants. But there are threats: Firstly, all modifications made to the participation list need to be checked so that no illegitimate voters can be added, and secondly, the identification system should be both trusted and secure so that a voter's account cannot be stolen or used by an intruder. Building such an identification system is a complex task in itself . However, because this sort of system is necessary for a wide range of other contexts, especially related to digital government services, researchers believe it is best to use an existing identification system, and the question of creating one is beyond the scope of work.

UNREUSADILITY

At first, glance, implementing unreusability may seem straightforward—when a voter casts their vote, all that needs to be done is to place a mark in the participation list and not allow them to vote a second time. But privacy needs to be taken into consideration; thus, providing both unreusability and voter anonymity is tricky. Moreover, it may be necessary to allow the voter to re-vote, making the task even more complex. A brief overview of unreusability techniques will be provided below in conjunction with the outline on implementing privacy.

PRIVACY

Privacy in the context of online voting means that no one except the voter knows how a participant has voted. Achieving this property mainly relies on one (or more) of the following techniques: blind signatures, homomorphic encryption, and mix-networks . Blind signature is a method of signing data when the signer does not know what they are signing. It is achieved by using a blinding function so that blinding and signing functions are commutativeBlind (Sign(message))=Sign(Blind(message)). The requester blinds (applies blinding function to) their message and sends it for signing. After obtaining a signature for a blinded message, they use their knowledge of blinding parameters to derive a signature for an unblinded message. Blind signatures mathematically prevent anyone except the requester from linking a blinded message and a corresponding signature pair with an unblinded one.

The voting scheme proposed by Fujioka, Okamoto, and Ohta in 1992 uses a blind signature: An eligible voter blinds his ballot and sends it to the validator. The validator verifies that the voter is allowed to participate, signs the blinded ballot, and returns it to the voter. The voter then derives a signature for the unblinded vote and sends it to the tallier, and the tallier verifies the validator's signature before accepting the ballot.

Many online voting protocols have evolved from this scheme, improving usability (in the original method, the voter had to wait till the end of the election and send a ballot decryption key), allowing re-voting, or implementing coercion resistance. The main threat here is the power of the signer: There must be a verifiable log of all emitted signatures; this information logically corresponds to the receiving of a ballot by the voter, so it should be verified that only eligible voters receive signatures from the signer

. It should also be verifiable that accounts of voters who are permitted to vote but have not taken part in voting are not utilized by an intruder. To truly break the link between voter and ballot, the ballot and the signature need to be sent through an anonymous channel .

Homomorphic encryption is a form of encryption that allows mathematical operations to be performed on encrypted data without decryption, for example, the addition Enc(a) + Enc(b) = Enc(a + b); or multiplication Enc(a) × Enc(b) = Enc(a × b). In the context of online voting, additive homomorphic encryption allows us to calculate the sum of all the voters' choices before decryption.

FAIRNESS

Fairness in terms of no one obtaining intermediate results is achieved straightfor- wardly: Voters encrypt their choices before sending, and those choices are decrypted at the end of the voting process. The critical thing to remember here is that if someone owns a decryption key with access to encrypted decisions, they can obtain intermediate results. This problem is solved by distributing the key among several keyholders . A system where all the key holders are required for decryption is unreliable—if one of the key hold- ers does not participate, decryption cannot be performed. Therefore, threshold schemes are used whereby a specific number of key holders are required to perform decryption. There are two main approaches for distributing the key: secret sharing, where a trusted dealer divides the generated key into parts and distributes them among key holders (e.g., Shamir's Secret Sharing protocol); and distributed key generation, where no trusted dealer is needed, and all parties contribute to the calculation of the key (for example, Pedersen's Distributed Key Generation protocol).

SOUNDNESS AND COMPLETENESS

On the face of it, the completeness and soundness properties seem relatively straight- forward, but realizing them can be problematic depending on the protocol. If ballots are decrypted one by one, it is easy to distinguish between valid and invalid ones, but things become more complicated when it comes to homomorphic encryption. As a single ballot is never decrypted, the decryption result will not show if more than one option was chosen or if the poll was formed so that it was treated as ten choices (or a million) at once. Thus, we need to prove that the encrypted data meets the properties of a valid ballot without compromising any information that can help determine how the vote was cast. This task is solved by zero-knowledge proof. By definition, this is a cryptographic method of proving a statement about the value without disclosing the value itself. More specifically, range proofs demonstrate that a specific value belongs to a particular set in such cases..

VI. SECURITY AND REQUIREMENTS FOR I-VOTING SYSTEM

Suitable electronic voting systems should meet the following electronic voting requirements. Figure shows the main security requirements for electronic voting systems.

AUDITABILITY AND ACCURACY

Accuracy, also called correctness, demands that the declared results correspond pre- cisely to the election results. It means that nobody can change the voting of other citizens, that the final tally includes all legitimate votes , and that there is no definitive tally of invalid ballots.

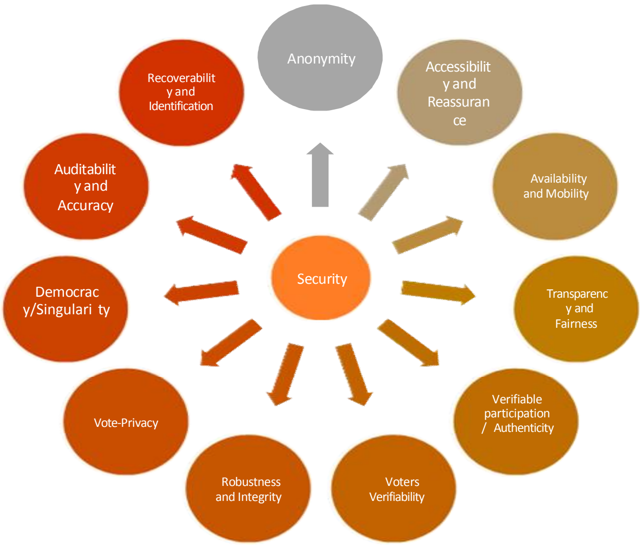
Anonymity
Accessibilit y and Reassuran ce
Availability and Mobility
Transparenc y and Fairness
Verifiable participation / Authenticity
Voters Verifiability
Robustness and Integrity
Vote-Privacy
Democrac y/Singulari ty
Auditabilit y and Accuracy
Recoverabilit y and Identification
Security

Figure: Security requirements for I-Voting System

ANONYMITY

Throughout the polling process, the voting turnout must be secured from external interpretation. Any correlation between registered votes and voter identities inside the electoral structure shall be unknown

DEMOCRACY/SINGULARITY

A "democratic" system is defined if only eligible voters can vote, and only a single vote can be cast for each registered voter. Another function is that no one else should be able to duplicate the vote.

VOTE PRIVACY

After the vote is cast, no one should be in a position to attach the identity of a voter with its vote. Computer secrecy is a fragile type of confidentiality, which means that the voting relationship remains hidden for an extended period as long as the current rate continues to change with computer power and new techniques.

ROBUSTNESS AND INTEGRITY

This condition means that a reasonably large group of electors or representatives cannot disrupt the election. It ensures that registered voters will abstain without problems or encourage others to cast their legitimate votes for themselves. The corruption of citizens and officials is prohibited from denying an election result by arguing that some other member has not performed their portion correctly

LACK OF EVIDENCE

While anonymous privacy ensures electoral fraud safeguards, no method can be assured that votes are placed under bribery or election rigging in any way. This question has its root from the start

TRANSPERANCY AND FAIRNESS

It means that before the count is released, no one can find out the details. It avoids acts such as manipulating late voters' decisions by issuing a prediction or offering a significant yet unfair benefit to certain persons or groups as to be the first to know.

VIII. CONCLUSION

On the research of various voting systems we analysed the security risk that could harm the integrity and confidentiality of the voting process. In these research exercises, we conceive a testing methodology, improved new tools for the security analysis and suggest a new idea of the voting system. The goal of this research is to analyze and evaluate current research on blockchain- based electronic voting systems. The article discusses recent electronic voting research using blockchain technology. The blockchain concept and its uses are presented first, followed by existing electronic voting systems. Then, a set of deficiencies in existing electronic voting systems are identified and addressed. The blockchain's potential is fundamental to enhance electronic voting, current solutions for blockchain- based electronic voting, and possible research paths on blockchain-based electronic voting systems. Numerous experts believe that blockchain may be a good fit for a decentralized electronic voting system.

Furthermore, all voters and impartial observers may see the voting records kept in these suggested systems. On the other hand, researchers discovered that most publications on blockchain-based electronic voting identified and addressed similar issues. There have been many study gaps in electronic voting that need to be addressed in future studies.

REFERENCES

[1]. Prof. Anisaara Nadaph, Rakhi Bondre, Ashmita Katiyar, Durgesh Goswami, Tushar Naidu "An Implementation of Secure Online Voting System"

[2]. Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan, NED University of Engineering and Technology, Pakistan "Secure Digital Voting System based on Blockchain Technology"

[3]. Liu, Y.; Wang, Q. An E-voting Protocol Based on Blockchain. IACR Cryptol. Eprint Arch. 2017, 2017, 1043.

[4]. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488.

[5]. Racsko, P. Blockchain and Democracy. Soc. Econ. 2019, 41, 353–369.

[6]. Yaga,D.; Mell, P.; Roby, N.; Scarfone, K. Blockchaintechnology overview. arXiv 2019, arXiv:1906.11078.

[7]. The Economist. EIU Democracy Index. 2017. Available online: https://infographics.economist.com/2018/DemocracyInde x/ (accessed on 18 January 2020).