iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71401

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Blockchain-Based Distributed Electronic Voting System Ensuring Privacy and Integrity through Smart Contracts

Mr. C. Gokul[1], Mr. D. Gokul[2], Mr. S. Jeeva[3], Mr. SS. Girikarthikeyan[4], Mrs. S. Dhanalakshmi[5], Mr. A. Gopi[6]
Computer Science and Engineering, Muthyammal Enginnering College, Rasipuram, Namakkal, Tamilnadu, India

Abstract: Traditional voting systems face significant challenges, including susceptibility to fraud, lack of transparency, and privacy concerns. Centralized electronic voting systems, while improving accessibility, often suffer from vulnerabilities such as tampering, single points of failure, and insufficient auditability. This project proposes a blockchain-based distributed electronic voting system that leverages smart contracts to ensure voter privacy, ballot integrity, and decentralized verification. The system employs cryptographic techniques such as zero-knowledge proofs (ZKPs) to anonymize voter identities while maintaining a verifiable audit trail on an immutable blockchain ledger. Smart contracts automate vote tallying, enforce voting rules (e.g., eligibility checks, one-vote-per- voter), and ensure tamper-proof execution of electoral processes. A permissioned blockchain network enhances scalability and reduces energy consumption compared to public blockchains. The system also incorporates multi-factor voter authentication and end- to-end encryption to safeguard against unauthorized access. By decentralizing control and enabling real-time transparency, this solution addresses critical flaws in existing systems, reduces electoral fraud, and strengthens public trust in democratic processes. The proposed architecture is implemented using Hyperledger Fabric for blockchain operations and Ethereum-based smart contracts, ensuring high performance, security, and compliance with electoral regulations.

I. INTRODUCTION

Electoral integrity is a cornerstone of democratic governance, yet traditional voting systems—ranging from paper ballots to electronic voting machines (EVMs)—are plagued by inefficiencies and vulnerabilities. Paper-based systems are labor-intensive, prone to human error, and lack real-time transparency, while centralized EVMs risk tampering, hacking, and opaque audit processes [7, 12]. Recent incidents of electoral fraud and disputes over vote counts underscore the urgent need for secure, transparent, and privacy-preserving voting mechanisms. Blockchain technology, with its decentralized, immutable, and transparent ledger, offers a transformative solution to these challenges. By distributing control across a network of nodes, blockchain eliminates single points of failure and ensures that no single entity can alter recorded votes. Smart contracts further enhance security by automating critical processes such as voter authentication, ballot casting, and tallying, thereby reducing human intervention and bias [3, 9]. However, existing blockchain voting prototypes often struggle to balance privacy with auditability, as public blockchains may expose voter identities through transactional metadata [5]. This project introduces a blockchain-based electronic voting system that integrates privacy-enhancing technologies (PETs) such as ZKPs and ring signatures to anonymize voter identities while preserving the ability to verify election outcomes. The system operates on a permissioned blockchain, ensuring scalability and regulatory compliance. By combining decentralized governance with cryptographic security, this solution aims to revolutionize electoral processes, ensuring fairness, integrity, and universal accessibility.

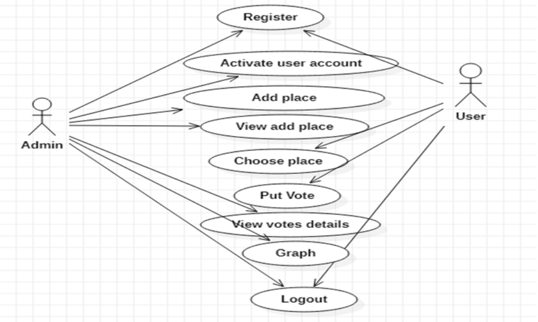

Figure 1 – Use Case Diagram

In past few years technology has advanced so far away that digitization and automation has emerged on every aspects of human life, society and nation. Web technologies and networking have improved in a radical manner. Today different online contests are arranged by various companies. In this type of contests, online voting plays an important role. Different social media are providing different features (LIKE, hashtag, favorites). But in this types of contests, a big question has raised- "Is the system secured enough to held fail voting?" Because the voting result can be manipulated in various ways.

In online voting, it is very important to make a safe and secure environment to make the competition perfect and fair. For proper voting, a secure system is essential. In our research we have shown the flaws of online voting system in different social media, product review systems and voting forms. It is challenging job to make a system secured for online voting. There are some trade offs towards a secured system. For example, a system can be secured from bots but it will decrease user friendliness. And it leads to lessen popularity of that particular competition. There are no such effective solutions to detect fake IDs. The problems regarding online voting in not organized and explained so far. That leads our interest to study the cases to find out the reasons behind the security issue. But these types of manual voting are causing lots of manipulations on vote casting and riots occurred. With the emerging advantage of technology, now it's possible to arrange National Election via online. That can erase the manipulation. But there are flaws in online voting system. So, national election cannot be arranged online so far. Before this, a secure online voting system essential. Our motivation behind this research was to find out the flaws behind online competition. In this paper we have discussed five cases and found the reasons behind the unfair competitions on online. As, digitalization is evolved on every aspect, security is the burning issue here. As elections have to be fair and proper leader must have to win for the welfare for the nation and society, online election also have to be more secure than manual voting. Our focus on this paper is to mark the problems and flaws on online security for fair voting that have to be eradicated.

II. LITERATURE SURVEY

Our paper deals with online voting system that facilitates user(voter), candidate and administrator (who will be in charge and will verify all the user and information) to participate in online voting. our online voting system is highly secured, and it has a simple and interactive user interface. The proposed online portal is secured and have unique security feature such as unique id generation that adds another layer of security (except login id and password) and gives admin the ability to verify the user information and to decide whether he is eligible to vote or not. It also creates and manages voting and an election detail as all the users must login by user name and password and click on candidates to register vote. Our system is also equipped with a chat bot that works as a support or guide to the voters, this helps the users in the voting process. The proposed system is built with a strong emphasis on security and usability. It features a simple and interactive user interface to ensure a smooth experience for all users. To enhance security beyond the standard login credentials of username and password, the system introduces a unique ID generation mechanism. This additional layer of security prevents unauthorized access and ensures the authenticity of each voter. The administrator leverages this feature to verify users' identities and determine their eligibility to vote, further strengthening the integrity of the voting process.

Security in the sense that voter high security password is confirmed before the vote is accepted in the main database of Election Commission of India. The additional feature of the model is that the voter can confirm if his/her vote has gone to correct candidate/party. In this model a person can also vote from outside of his/her allotted constituency or from his/her preferred location.

We have stated several case studies concerning online voting manipulation. Case studies data are analyzed to discover how computer technology is used to manipulate voting in Social Media for future research. The study found that, there are many potential Weaknesses that should be treated as highly hazardous for online voting

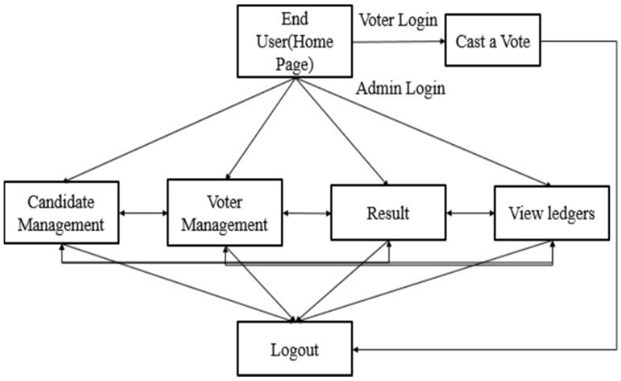

Figure 2 – Architecture

III. SYSTEM

A. Existing System

The existing system is manual and the paper based voting which is voted on paper and counted manually. The electronic tabulation brings new kind of voting system in which the electronic cards with all candidates symbol is marked manually and this can be counted electronically. The electronic voting systems are now different types known as the punch card, mark sense and the digital pen voting systems. The Electronic Ballot Marker makes the voter easier to vote by providing the selections on the display to vote present on the electronic machine.

The direct recording electronic voting machine is one which provides the display that can be start when the voter touches the display consists of the mechanical and electro optical buttons, software that accepts the vote and possesses a image or symbol on the display.

The electronic ballots are connected with the central ballot systems which directly accept and get the updated record of all ballots. The central ballot system applies the Precinct count method which calculates the all votes from the ballots present at polling centers. The results are immediate.

Disadvantages

- Manual work
- Low performance
- Requires more time .

B. Proposed System

The online voting system is for the citizens from all over India that consists of the data and information. In this project, user should vote for their candidate by using only the aadhar card. For that user needs to register first and then he/she will receive the OTP through mobile number. Then only user can login to the application. Then he/she can vote for their decided candidate.

The database of the Voter’s information

1) Voter’s Id
2) Calculation of total votes
3) Checking information by the voter
4) Remove wrong information
5) The information immediately transfers to Election Commission.

Advantages

- Fast and easy service.
- The online voting system provides a less time consuming.
- It reduces the paper work and makes the work less tedious for Election Commision.
- It is a better way for voting.
- By this voting percentage will increase drastically.
- Voter has no need to go to any polling booth, so it is easy to use

IV. MODULES

A. Module Description

In this project has two modules:

1) Admin

- Login the account with correct username and Password
- View all the active and in active users
- Admin can add the party name with the full details
- View all the candidate list
- View the vote result based on location
- View the result based on their voteing in graph method
- Logout

2) User

- Register the account with the basic information
- After authorize by admin ,user can login the account with correct username and password
- User have hash key verification and fingerprint verification, after all type verification user can login the account
- User can choose location and can on your vote
- You are already vote means can't vote again same
- Logout

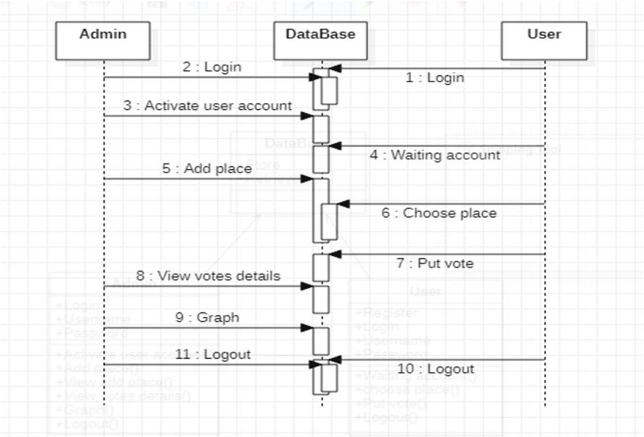

Figure 2 – Sequence Diagram

V. CONCLUSION

This paper describes the proposed model for online voting system for India. The proposed system is much secure and efficient than the traditional voting system. Manipulation of votes and delay of results can be avoided easily. A unique AADHAAR identity is the center point of our proposed model.

It leads to the easier verification of both voters and candidates. In the proposed framework, we have tried to build a secure online voting system that is free from unauthorized access while casting votes by the voters. The server aspects of the proposed system have such distribution of authority that server does not enable to manipulate the votes. It is expected that the proposed online voting system will increase the transparency and reliability of the existing electoral system.

The challenge of developing electronic voting systems is not only security but also protecting the secrecy of the ballot, a bedrock principle of free and fair elections. Currently there is "no known technology that can guarantee the secrecy, security, and verifiability of a marked ballot transmitted over the Internet." Online voting presents numerous vulnerabilities and is fundamentally insecure. There is potential for unobserved vote manipulation as well additional security vulnerabilities including potential denial of service attacks, malware intrusions, and privacy concerns.

REFERENCES

[1] Aakash Suryavanshi, "Online Voting system",IEEE,2020.
[2] David Evans and Nathanael Paul, "Election security: Perceptio and reality", IEEE Security & Privacy, vol. 2(1), Jan. 2004, pp. 24-31.
[3] David Jefferson, Aviel D. Rubin, Barbara Simons, and DavidWagner, "Analyzing Internet voting security", Communications of the ACM, vol. 47(10), Oct. 2004, pp.
[4] David L. Dill, Bruce Schneier, and Barbara Simons, "Voting and technology: Who getsto count your vote?", Communications of the ACM, vol. 46(8), Aug. 2003, pp. 2931.
[5] Executive Summary of "Genesis and Spread of Maoist Violenc and Appropriate State Strategy to Handle it", Bureau of Police Research and Development, Ministry of Home Affairs, New Delhi http://en.wikipedia.org/wiki/Electronic_ voting.
[6] Himanshu Agarwal, "Online voting system for India based on AADHAAR ID",IEEE,2017.
[7] http://newindianexpress.com/states/ Andhra Pradesh/Maoists- strike-fear-make-off-with- poll-papers-in-agency/2013/07/15/ article1684243. Ece.
[8] MD. Shamsur Rahim , "Analyzing Online Voting Systems for Flaw Detection",IEEE,2015.
[9] Rebecca Mercuri "Statement on electronic voting" http://www.notable software.com/RMstatement.html, 2007.
[10] Tadayoshi Kohno, Adam Stubblefield, Aviel D.Rubin, Dan S. Wallach, "Analysis of an Electronic Voting System", Johns Hopkins University Information Security Institute Technical Report, TR-2003-19, July 23, 2003.