

Online Voting System Using Fingerprint sensor and Blockchain

Ridham¹, Prakhar Sharma², Aditya Batra³, Prof. Purna Sharma⁴

¹Student, Maharaja Agrasen Institute of Technology

²Student, Maharaja Agrasen Institute of Technology

³Student, Maharaja Agrasen Institute of Technology

⁴Asst. Professor, Maharaja Agrasen Institute of Technology

Abstract - An online voting system also referred to as an online polling system or e-voting system is an emerging tool to maintain integrity and rightfulness to one's fundamental rights while casting their preference in the elections. Digitalization has been proven to be a helping hand to mankind with emerging technologies like blockchain, which is widely adopted worldwide to ensure end-to-end authentication, encryption, and verification advantages we have used Aadhar Id and fingerprint sensor in this project research to increase the integrity and security factors. Here it serves as a secure method to carry out election processes. We tend to carry out this sensitive process in the decentralized distributive system without any outer alterations to the data stored in blocks and hashes thus helping the users to cast votes remotely in a hassle-free, time-saving and paperless manner, thus reducing insufficiency and malpractices that have widely been seen in a traditional ballot or Electronic Voting Machine (EVM) systems.

Key Words: Blockchain, Digitalization, Decentralized, Encryption, integrity, Authentication, Aadhar id, Electronic Voting Machine

1. INTRODUCTION

Voting is one of the oldest methods to elect a supreme head in any institution, committee, or political body. In most democratic countries like India, voting has been widely adopted over the years to create an atmosphere of integrity and rightfulness where people have the right to choose a representative who can serve their demands [3]. The most adapted traditional way of electing a leader over the years has been casting votes where people gather physically at polling booths and elect a member.

1.1 Problem with existing system

The major problem which is mostly seen in this traditional method where people cast votes using Electronic Voting Machines (EVMs) is the usage of malpractices influencing people and getting votes, forcefully threatening people, lack of privacy, security, compliance issues, and unbothered citizens [2].

1.2 Online Voting as a solution

Blockchain is an efficient emerging technology that works on end-to-end encryption. Due to its intrinsic ability to preserve anonymity, maintain a decentralized and publicly distributed ledger of transactions across all nodes, and play a significant role in the field of electronic voting, by storing data in blocks that cannot be altered until the data gets delivered as the information thus maintaining security, integrity, and privacy of users in such sensitive processes. With votes being cast remotely from any place, without any biased interference saves time, maintains fundamental rights, and motivates people to take part in the process.

1.3 Scope

For verification, the person's Fingerprint will be scanned on the client-side and matched one-to-one at the servers with the data extracted from the local database. We used Fingerprints for authentication because processing Fingerprints is faster and better than other biometric data. Moreover, by using Fingerprints it is ensured such fake entries are blocked right at the very beginning [8]. Thus, the online voting system is an approach to bring anonymity, integrity, productivity, and liberty to an individual ensuring security and accessibility to the people to take part in elections and vote freely with their own decision.

2. LITERATURE SURVEY:

Block chain was first introduced by Satoshi Nakamoto (a pseudonym), who proposed a peer-to-peer payment system that allows cash transactions through the internet without relying on trust or the need for a financial institution. Block chain is secure by design, and an illustration of a system with a high intricate failure forbearance. E-voting is an implicit result to the lack of interest in advancing amongst the youthful tech smart population. For e-voting to come more open, transparent, and singly auditable, an implicit result would be base it on blockchain technology. Blockchain technology has a lot of pledge; still, in its current state it might not reach its full eventuality.

Gaby G. Dagger, Mateo Milinkovic, and Jordan Mahler (2018) deal with Voting as a fundamental part of democratic systems, it gives individuals in a community the faculty to voice their opinion. In recent times, name turnout has

lowered while enterprises regarding integrity, security, and availability of current voting systems have escalated. E-Voting was introduced to address those concerns; however, it is not cost-effective and still requires full supervision by a central authority. The Blockchain is an emerging, decentralized, and distributed technology that promises to enhance different aspects of many industries.

Many organizations such as [1] have created their own polling website where they can cast votes among their own selected group of veterans and military family members to elect the next generation of poll workers. There are many such websites that allow organizations and people to cast votes at low levels.

Past studies show that an online voting system was suggested. It was primarily built using python and other programming languages. It allowed users to cast votes by simply logging into their accounts with their user ids and casting votes. But this doesn't ensure much privacy and authenticity to one's identity [9].

Pashine, naive and kelapure [4] proposed an android platform for online voting system. This application provides diversion of long process also provide security to the voter and its voter comfort system voter no need to go polling booth easily vote for candidate in hometown itself. And also provide the option of gesture recognition but authentication is the problem of android platform. In this application which is partitioned into three panels Admin Panel, Candidate Panel and Voter Panel.

Khasawneh [5] Proposed An E-Voting System for Biometric Security Is Providing A Two Sided Solution Such As Server And User Side. After casting the vote system will induce hardcopy for voter and also induce unique number. This unique number and voter name and identification number is secured. All content is stored in special box. This box is secured box. This information is habituated for vindicating the vote Before Stored in Final Database. This side copy is printed with unique barcode that can be easily readable automatically and scanned then randomly choose one cop, then this copy is tested. This two-sided process providing verification and correctness for the system.

Firesl. Hazzan, Seifeddine Kadar(6) this paper deals with the design and development of a web- grounded voting point in order to give a high performance with high security to the voting system also we use web technology to make the voting system more practical. The new design is proposed an election for a university for selecting the president of the university. The proposed EVS allows the choosers to overlook their point, which is also matched with an formerly saved image within a database. Developed Web- grounded Voting System using Fingerprint Recognition. This system has handed an effective way to cast votes, free of fraud, and make the system more responsible, profitable and fast.

We've used Minutiae- grounded point identification and matching with high delicacy.

Another research used facial detection to increase security measures but it doesn't completely justify one's identity and anonymity while electing a leader. It doesn't ensure fair means and may cause ambiguity issues. Earlier it wasn't much validated which could ensure the user to check if their vote has been successfully done or whether they are eligible or not, thus leaving many important factors unnoticed.

As technology advances, many countries have now opted for electronic voting systems. Any voting system must follow principles of translucency and equity in order to achieve fairness. The blockchain mechanism employs a distributed architecture and all these researches somewhat lack the anonymity, authenticity and realness of user which can be overcome using combination of different features like using Aadhar id, confidential details and most importantly fingerprint sensor which ensures integrity and realness of the user.

3. METHODOLOGY:

This digital voting system is a platform that enables only authentic and eligible users to cast their votes in the elections. The user is provided to log in first to the window with the right credentials. He would register with the phone number or Aadhar card id or voter id issued to him. Once the user is found authentic and eligible, that is, the system holds his data, he meets the age criteria, and citizenship of the region or nation he is casting votes for, he is moved to further process. It is being worked to implement the fingerprint sensor so as to increase the authenticity and security of the system. We have considered 2 main modules which are as follows:

A. Admin- The admin module is divided into 5 components-

1. Dashboard-It will contain various charts to display information such as number of parties, no. of voters etc.
2. Add seeker- In this point of admin, he can add campaigners who are standing in the election. After seeker is added it'll be displayed on the stoner side.
3. Create Election- This feature of admin will allow him to create election. A user can cast his vote only after the election is created by admin. A user can cast vote between the start date and end date.
4. Election Details- In this section admin can update election details such as start date, end date etc.
5. Candidate Details- In candidate details all the candidates added by admin will be displayed. Admin can modernize the seeker details if incase a wrong entry is done.

B. User- The user module is divided into 4 components-

1. Dashboard- The user dashboard contains information about parties and their candidates. A user can see all the information about candidate.
2. Voter Register- In this section first user will have to register himself only then he will be able to cast his vote.
3. Voting Area- After user is registered, then only he will be directed to this page and then he can cast his vote.
4. Results- In this component the user will be able to see the results of the election.

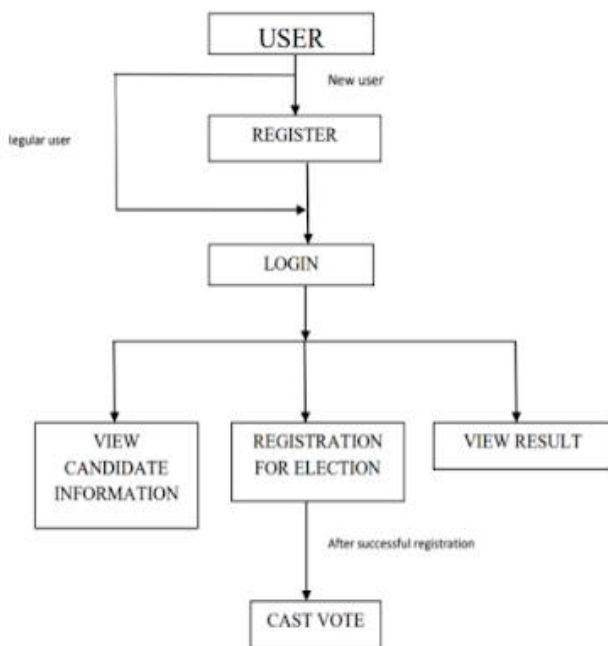


Fig -1: User Flow Diagram

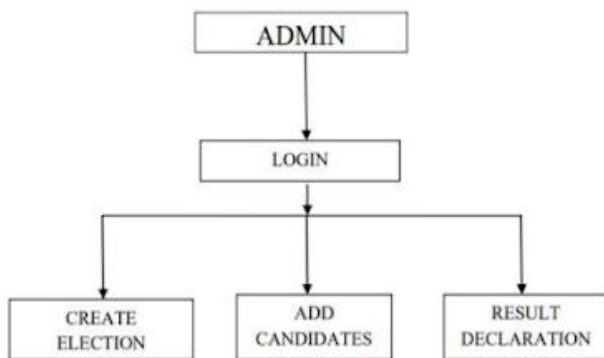


Fig -2: Admin Flow Diagram

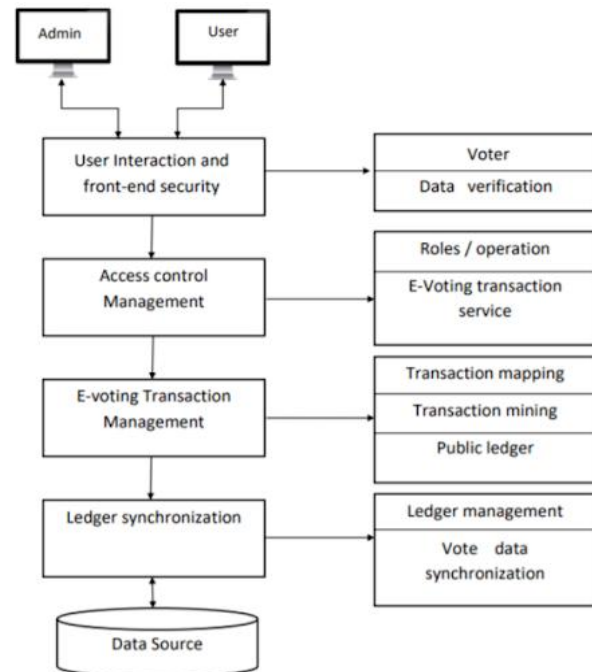


Fig -3: Research Methodology Diagram

3.1 Algorithms:

Minutiae Based Algorithm

In this we use two algorithms: minutiae-extraction algorithm (fingerprint detection) and minutiae-matching (matching fingerprint i.e. input fingerprint and database fingerprint) algorithm.

a. Minutiae Extraction

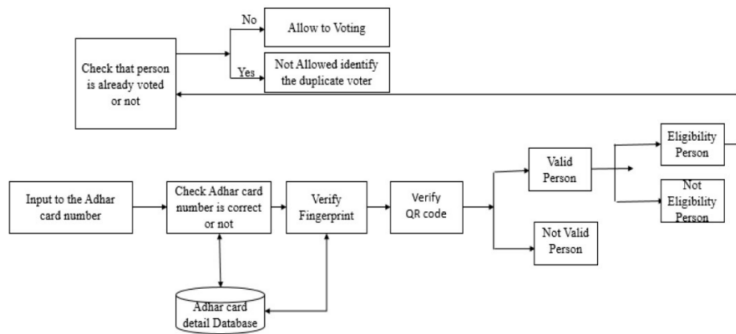
Fingerprint authentication is based on minutiae patterns matching. Minutiae extraction consisting three components:

- i. Orientation field estimation
- ii. Ridge extraction
- iii. Minutiae extraction and post processing

b. Minutiae Matching

We can match fingerprint by different strategies, such as point pattern matching, image-based matching, ridge pattern matching, graph-based scheme, etc. The point pattern matching is the minutiae matching. a minutia matching is decomposed into two stages:

- i. Alignment stage
- ii. Matching stage



The process can further proceed in another section where the user can cast vote according to his choice using the MetaMask wallet. Once the vote is cast, the user receives a notification of the same or can see the progress in the status section of the system.

Once the vote is cast with one id/ number/ Aadhar id, the voter gets ineligible to cast vote again for the same process. This maintains homogeneity and anonymity.

The system can be used by several other members who may be from the same family, team, or group but with their own IDs and Aadhar IDs which makes the system distributive while maintaining privacy.

The user doesn't need to visit any pooling booths which will save a lot of time, reduce workload, and can prevent any possible interference which could lead to biased decisions thus preserving one's fundamental rights and integrity to personal information.

3.2 Fingerprint Verification:

A person must have a valid UID number in order to be authenticated. The local database records will be examined first before the number is used. The central repository will be searched if it cannot be located. A one-to-many match is involved. Naturally, the person won't be able to participate in the voting procedure if their number cannot be located in the main database. This record is taken out of the local database and forwarded to the servers that handle authentication for further processing. For verification, the client-side fingerprint scan of the user will be compared one-to-one at the servers with the information taken from the local database. The local database is less stressed by this approach, and data throughput is increased. Because processing fingerprints is quicker and more accurate than processing other biometric data, we employ fingerprints for authentication. Aadhar information would also be insufficient to prove a person's genuine identity because it is simple to spoof them, but utilizing fingerprints ensures that bogus entries are stopped at the source [9].

3.3 Technologies Used:

The whole system is blockchain-based and is run on Ethereum (an open-source platform to create blockchain applications). We have also used smart contracts which hold the terms and conditions for certain applications to be built. These are the programs stored on the blockchain program which are allowed to run when certain conditions are met. Solidity is the high-level language on which the whole project is built. We know that any process that undergoes in a blockchain is considered a transaction and to carry out each step of the process which is referred to as a transaction here is achieved using the MetaMask wallet. It generates passwords enabling only one current user to access the system which makes it a secure platform while undergoing such sensitive processes. Since the transactions require actual money, Ganache is used as a local RPC which provides 10 accounts to check or test the transaction. Truffle is the framework suite that is used in Ethereum to interact with compiled smart contracts in an easier and more effective manner.

4. FUTURE SCOPE:

Online Voting techniques can be greatly adapted in nearby future for big decision makings like elections in any country, which will allow citizens to live a balanced social and personal life. It can replace the current EVMs and with the fingerprint sensor, this model can become more reliable, thus ensuring only authentic and eligible users cast their votes. Some of the important features that can be implemented are:

- 1) Improved security measures: You could focus on developing advanced security measures, such as encryption, biometric authentication, and other technologies, to protect against cybersecurity attacks and ensure the integrity of the voting process.
- 2) Enhanced accessibility: You could design your app to be more accessible for people with disabilities, for example by offering features such as text-to-speech or visual aids for people with vision impairments.
- 3) Improved convenience: You could offer features such as automatic ballot scanning or the ability to cast votes from multiple devices to make the voting process more convenient for users.
- 4) Integration with other systems: You could integrate your app with other systems, such as voter registration databases or candidate information portals, to provide a more seamless and convenient voting experience.
- 5) Additional language support: You could translate your app into multiple languages to make it more accessible to non-English speakers.

6) Verification and auditability: You could incorporate features such as voter verification and ballot tracking to enhance the transparency and auditability of the voting process.

7) Improved user interface: You could focus on designing a more user-friendly interface to make it easier for people to navigate and use your app.

8) Advanced analytics: You could equip your app with advanced analytics capabilities to help electoral authorities better understand voter behavior and preferences.

It's also important to conduct market research to understand the needs and preferences of potential users, as well as to identify any gaps in the current offerings that your app could fill.

5. CONCLUSION:

Digitalisation and Blockchain together in a single framework is found an efficient way to maintain anonymity, integrity, privacy, and basic fundamental rights of any user or citizen of any nation while carrying out the process of voting which is generally compromised in current traditional methods of ballots and EVMs. By using different configuration techniques like including Aadhar Id and fingerprint sensors while casting votes, it ensures authenticity and integrity. The status of votes on one's own system ensures privacy and reliability to be a productive and responsible citizen. An online voting system would lower the cost of elections conducted on paper and boost voter turnout. By using this technology, additional votes can be cast, and the results of those votes are accurately, permanently, securely, and publicly recorded.

REFERENCES:

- [1] Himanshu Agarwal and G.N. Pandey "Online Voting System for India Based on AADHAAR ID" 2013 Eleventh International Conference on ICT and Knowledge Engineering
- [2] Smita B. Khaimar, P. Sanyasi Naidu, Reena Kharat "Secure Authentication for Online Voting System"
- [3] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi "Online Voting System Powered By Biometric Security" 2011 Second International Conference on Emerging Applications of Information Technology
- [4] F. Hai, M. N. Kreeger, B. Randell, D. Clarke, S. F. Shahandashti, and P.H.-J. Lee. Every vote counts: Ensuring integrity in large-scale electronic voting. *USENIX Journal of Election Technology & Systems*, 2(3):1-25, 2014.
- [5] Feng Hai and Peter Y A Ryan (Eds). Real-world Electronic Voting: Design, Analysis and Deployment, Series in Security, Privacy and Trust. CRC Press, 2016.
- [6] Divya G Nair, Binu. V.P, G. Santhosh Kumar, "An Improved E-voting scheme using Secret Sharing based Secure Multi-party Computation", arXiv: 1502.07469v1 [cs.CR] 26 Feb 2015
- [7] Roberts, C. Biometric attack vectors and defences. *Comput. Secur.* **2007**, *26*, 14–25. [[Google Scholar](#)] [[CrossRef](#)] [[Green Version](#)]
- [8] Páez, R.; Pérez, M.; Ramírez, G.; Montes, J.; Bouvarel, L. An Architecture for Biometric Electronic Identification Document System Based on Blockchain. *Future Internet* **2020**, *12*, 10. [[Google Scholar](#)] [[CrossRef](#)] [[Green Version](#)]
- [9] Nimje, R.; Bhalerao, D. Blockchain Based Electronic Voting System Using Biometric. In Proceedings of the International Conference on Sustainable Communication Networks and Application, Erode, India, 30–31 July 2019; pp. 746–754. [[Google Scholar](#)]
- [10] Pawade, D.; Sakhapara, A.; Badgujar, A.; Adep, D.; Andrade, M. Secure Online Voting System Using Biometric and Blockchain. In *Data Management, Analytics and Innovation*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 93–110. [[Google Scholar](#)]
- [11] Odelu, V. IMBUA: Identity Management on Blockchain for Biometrics-Based User Authentication. In Proceedings of the International Congress on Blockchain and Applications, Ávila, Spain, 26–28 June 2019; pp. 1–10. [[Google Scholar](#)]
- [12] Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *J. Netw. Comput. Appl.* **2019**, *125*, 251–279. [[Google Scholar](#)] [[CrossRef](#)]
- [13] Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; 2008; Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 1 June 2020).
- [14] Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where is current research on blockchain technology? —A systematic review. *PLoS ONE* **2016**, *11*, e0163477. [[Google Scholar](#)] [[CrossRef](#)] [[PubMed](#)]
- [15] Multichain (2017) Open platform for Blockchain applications. Available at: www.multichain.com last accessed: December 2017.
- [16] McCorry, P., Shahandashti, S. F. and Hao, F. (2017) A smart contract for boardroom voting with maximum voter privacy in the proceedings of FC 2017.

[17] Kraft, D. (2015) Difficulty Control for BlockchainBased Consensus System, Peer-to-Peer Networking and Applications by Springer, March 2015

[18] Kadam, M., Jha, P. Jaiswal, S. (2015) Double Spending Prevention in Bitcoins Network, International Journal of Computer Engineering and Applications, August 2015

[19] Rosenfeld. M. (2017). Analysis of hashrate-based double-spending. [Online].

[20] Umut Can Çabuk¹, Eylül Adıgüzel², Enis Karaarslan² (2018); A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems; International Journal of Advanced Research in Computer and Communication Engineering. [Online].

[21] Aayushi Gupta¹, Jyotirmay Patel², Mansi Gupta¹, Harshit Gupta¹ (2017); Issues and Effectiveness of Blockchain Technology on Digital Voting; International Journal of Engineering and Manufacturing Science. ISSN 2249-3115 Vol. 7, No.1 (2017). [Online].

[22] Pavel Tarasov and Hitesh Tewari (2017); the Future of E-Voting; IADIS International Journal on Computer Science and Information Systems Vol.12, No. 2, pp. 148- 165 I. [Online].