A Trustworthy Voting Framework Using Aadhaar and Distributed Ledger Technology

B. Varun Kumar[1], M.Nikhil Kumar[2], T.Nithin Kumar[3], G.Janaki Ram[4], Ch.Lavanya[5], S. Shiva Prasad[6]
[1,2,3,4]*Student, Department of CSE(DataScience), MallaReddy Engineering college, Secunderabad*
[5]*Assistant Professor, Department of CSE(DataScience), MallaReddy Engineering college, Secunderabad*
[6]*Professor, Department of CSE(DataScience), MallaReddy Engineering college, Secunderabad*

***Abstract*—Voting is a fundamental process in a democratic system, but traditional voting methods face several challenges such as vote rigging, impersonation, lack of transparency, and high operational costs. To overcome these issues, this project proposes a secure online vote casting system using Aadhaar verification integrated with blockchain technology. In the proposed system, voter identity is verified using Aadhaar-based authentication to ensure that only eligible voters can participate in the election. Blockchain technology is used to store votes in an immutable and tamper-proof manner, which improves transparency and trust in the voting process. Once a vote is recorded on the blockchain, it cannot be altered or deleted, ensuring the integrity of election data. The system also prevents duplicate voting and enables accurate and faster vote counting. This approach aims to provide a secure, transparent, and reliable digital voting platform that can enhance voter participation and strengthen the electoral process.**

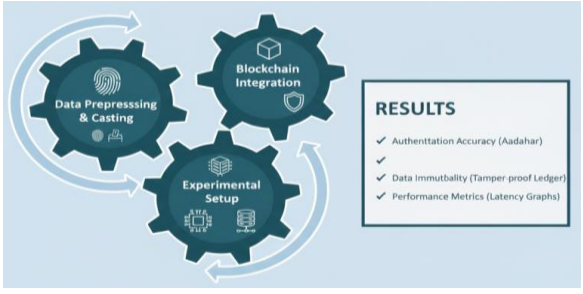
***Index Terms*—Online Voting System, Aadhaar Authentication, Blockchain Technology, Secure Vote Casting, Digital Voting, Data Security, E-Governance**

I. INTRODUCTION

The integrity and transparency of the voting process are cornerstones upon which modern democracy bases its representation of the collective will of its people in governance. In recent times, the domain of digital governance has been vying for a switch to e-voting systems, furthering ease and rapid tabulation of results. Yet, all the while, the challenge remains to provide an "End-to-End Verifiable" system that is resilient against manipulations by any form of centralized processing entity. Your research sits at the crossroads of E-Governance, Biometric Security, and Distributed Ledger Technology, dwelling upon how decentralized systems could replace traditional, vulnerable architectures so as to restore public trust in the electoral process.

Traditional voting, before the integration of high-level digital technologies, was heavily reliant on paper ballots or basic EVMs. Although these systems were an improvement over physical paper, they created important risks, such as centralized data storage where a single point of failure could compromise the integrity of an entire election. As mentioned in previous works, these traditional models often lack a transparent audit trail, which means that voters have no way to independently verify that their specific vote was counted exactly as cast without being altered by an intermediary or a "black box" system error.

Identity fraud is one of the issues that has persisted from the older electoral frameworks, taking the forms of "bogus voting" or voter impersonation. Where voter identification in such systems relies on manual checks by the polling officers through a physical ID card, this is a process fraught with human error, while proxy voting is often made possible. Studies into these older models suggest that without a robust automated link to a national biometric database, it is virtually impossible to guard against an individual's serial voting or to prevent the citation of a dead or absent citizen's credentials to



II. LITERATURE SURVEY

The transition to blockchain systems for the voting space is due to the vulnerabilities that are generally associated with traditional systems. It has been suggested that, in traditional systems, when data is stored in the hands of only one authority, there remains the “single point of failure” that can have an election compromised. By implementing the decentralized ledger system in the voting space, the strategy is to develop a platform in which no single authority can change the result. In earlier systems, the only issue that remains critical is the space that is consumed in terms of computation.

Another significant contribution in this area is multi-layered biometric authentication for confirming the identity of voters. Researchers have suggested making use of distinct biological characteristics like finger prints associated with individual ID cards like Aadhaar for ensuring that it is actually the same individual who stands in front of the voting booth or station. Hence, this method altogether removes any possibilities of vote proxy and identity spoofing. Although this method has several advantages regarding enhanced levels of security, one main disadvantage is associated with the complexity involved in its implementation due to its sensing technology that might be sensitive to its surroundings and thus may result in voters being deprived of their voting rights if it is not implementation-perfect.

However, further study has also focused on the effectiveness of two-factor systems in order to offer a further degree of security. The benefit in the "multimodal" security system lies in the near-perfect security standards in ensuring that there are no repliche votes or "bogus" polls. However, the challenge lies in the financial costs involved in the installment of adequate iris scanners in each local polling booth. This has often proved to be a rather expensive project in many developing countries, thus widening the gap between theoretical security standards and practical applications.

Some other studies have centered on the usage of One-Time Password (OTP) verification as a relatively more economical means of voter authentication in place of or in addition to the use of biometric hardware components. These researchers have used the mobile networks available in their region in an attempt to add a means by which voters can be verified remotely or through digital means with no need for hardware in the booth. A major drawback of this mechanism would be the vulnerability of cellular networks and the problem of "SIM swapping" or mobile hacking. A hacker could gainaccess to the voter’s mobile phone, thereby depriving the voter of the means of secure voting.

The implementation of the Ethereum blockchain and smart contracts developed using Solidity is an incredible development in the automation of voting rules. The researchers in this space have been able to prove that smart contracts have the ability to implement rules such as ensuring a vote by each voter can only count once without human involvement. The major advantage that this technology has concerning transparency is that it is indeed transparent. The major disadvantage, however, lies in what is referred to as “gas fees” or “transaction fees.” The issue with implementing such votes within the public blockchain setting is that it is very expensive during peak usage.

Research studies on data integrity have further emphasized the impact of decentralized storage systems as a mechanism to avoid the manipulation of electoral results. The network has managed to distribute the voting ledger among a vast number of nodes, ensuring that even when the attackers target several nodes, the result will not be altered because the majority consensus will maintain the original information stored. The flip side of this technology, which prevents the manipulation of electoral results, is that the system has latency when the number of nodes used is increased, which could slow down the voting process during a national election.

The implementation of IoT-based Electronic Voting Machines (EVMs) has offered a link between traditional voting and recording processes. These systems play an important role in these proceedings by transmitting all data in real-time to secured cloud servers, thus limiting access for local manipulation. A crucial limitation found with these IoT systems is that they are prone to Distributed Denial of Service (DDoS) attacks. If these systems are overwhelmed with these attacks, specifically on their connectivity to the internet, then the vote transmission system to blockchain within the polling station might become hindered.

The task of keeping voters anonymous while at the same time being completely audit-trail-friendly is

perhaps one of the toughest endeavors present within the existing body of literature. Several cryptographic approaches have been offered within this field by many authors and experts, some of the most popular of which include "zero knowledge proofs" that enable a method to authenticate that a vote is legitimate without having to disclose whose vote it is at all. Although this helps to preserve voters' secrecy and their right to a secret ballot, its "black box" nature may paradoxically end up undermining voters' trust because of its opaque complexity, even as its security is beyond questioning. However, due to the advancements and increases in the computations afforded by quantum computers, some of these scholars have moved on to the design of “quantum-resistant” blockchain voting systems.

Their significance lies within the application of post-quantum cryptography to protect the voting information. However, the weakness associated with these advanced systems is the huge processing capabilities required. Most of the current IoT technology voting systems do not possess the necessary specifications for processing this technology. Finally, feasibility studies at a larger scale suggest that, pragmatically, blockchain voting is efficient at a pilot scale, but scalability is a huge issue. Some scholars have made efforts to address scalability issues by developing "sharding" and "side chain" models, but in many cases, that comes at a cost to security as well. The challenge, in any case, is described by many as "trilemma," meaning having issues with speed, security, and decentralization simultaneously, until a scale is achieved where millions of votes could be processed at once without sacrificing either one of those three qualities, blockchain voting is an area of hot debate.

III. PROPOSED METHODOLOGY

The proposed methodology emphasizes the mitigation of the most crucial weaknesses of the traditional voting system, including bogus voting and the effects of tampering by the authorities, by making use of the concept of authentication through biometrics and a decentralized blockchain model. Thus, the proposed solution relies on Aadhar authentication and fingerprint authentication using IoT-enabled devices to make sure that only eligible voters are able to cast their votes.

To promote maximum transparency and accountability, the process employs smart contracts to automate rules in the election, hence ruling out the possibility of human error in the process. The vote cast in the process is considered an irrevocable transaction on the Ethereum network; hence, there is maximum accountability through the audit trail provided by the blockchain technology in this case.

3.1 System Architecture

The design of the proposed system features a secure, distributed network where physical polling centers are connected to a virtual, decentralized ledger. The user interface for voters to make their final choice of candidates is where IoT-based Electronic Voting Machines (EVMs) are installed. The EVMs are connected to fingerprint sensors, which further link to a secured cloud server containing the Aadhar biometric database.

The second tier is composed of a distributed network of nodes, where the fundamental election algorithm is implemented using the Ethereum blockchain. Additionally, smart contracts implemented in Solidity code handle the candidate registration, the validation of voters, and the computation of election results. This particular tier is important in ensuring that the votes cast cannot be manipulated by a failure point, since the vote is replicated on the entire nodes of the network immediately after casting.

In terms of the back-end layer, the application of the central cloud server is geared towards encrypting and storing Aadhar fingerprint templates and enabling data forwarding in real-time for all IoT devices. In addition, this layer comprises a monitoring component that is involved in creating graphs to measure latency in transaction processes of the blockchain technology. This system is highly secure in eliminating both physical and cyber threats.

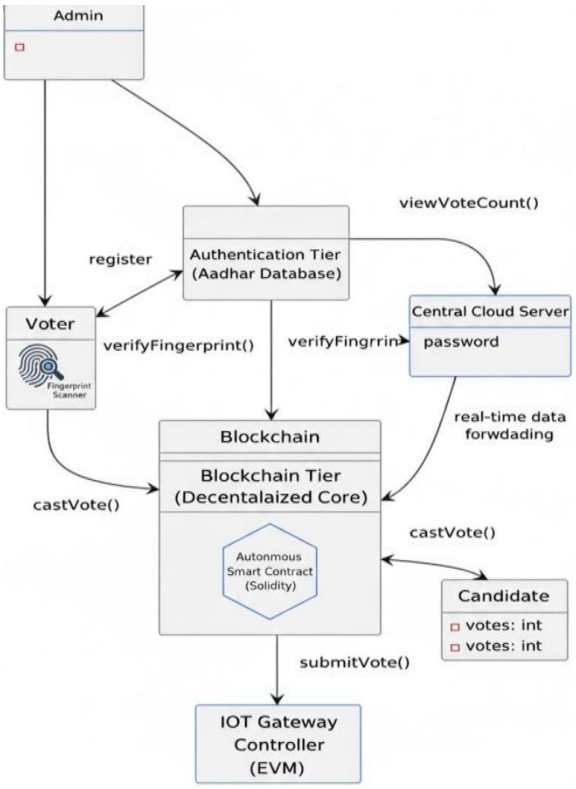


Figure.1 Flow chart of proposed system

3.2 Data Pre-processing

for this particular setup involves biometric feature extraction and normalization from the fingerprint scan of the voter. The process involves a voter placing a finger on a scanning device,

where the raw scan is then undergoes processing for minutia points extraction, which are then transformed into a mathematical model. The model is then encrypted before being posted to the cloud server, such that the biometric details of the user are never shown in clear form during the authentication process.

The second stage of preprocessing is the validation and verification of the credentials of the voter against the national Aadhar database. This stage involves checking the live biometric template against the database on the secure cloud, and if it matches, a result status is updated on the blockchain node that allows the vote because the person is authorized. Finally, the database is also checked on the smart contract with respect to the Aadhar ID number to see if the person voted before and thus not an attempt to vote twice.

After the identity is established, there is vote preprocessing in order to transform it to fit blockchain transaction requirements. The voter's decision is then matched with a transaction hash and a time stamp, which is subsequently encrypted with the public key of the smart contract. All such measures ensure that the data is in a formable state capable of being retained in the Ethereum blockchain, where it is secure and can be audited at all times during the voting process.

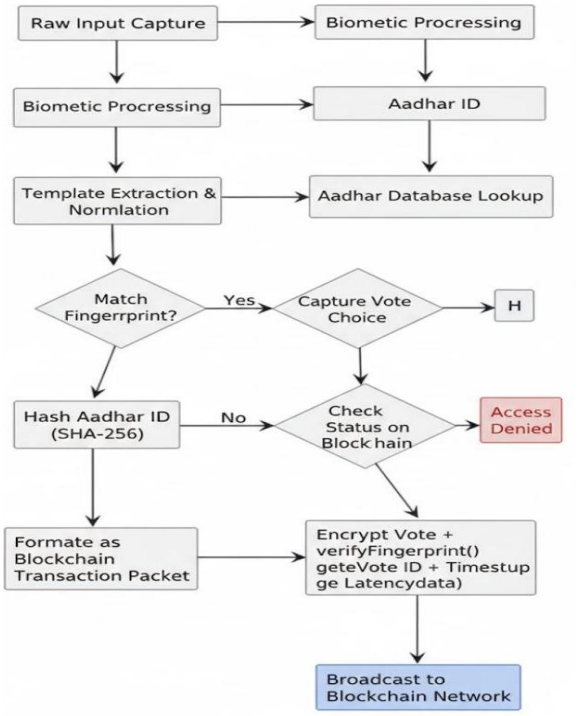


Figure.2 Sequence diagram of model

IV. EXPERIMENTAL SETUP AND RESULT

The lab work phase in this research will entail creating a setup in which the different components can interact with each other for a simulation of a secure election. Such a setup will involve the real-time biometric authentication of the votes and the recording of the votes in a decentralized system known as a ledger. It is through the setting of such special setups in the system that there will be a platform for evaluating the efficiency of voting using blockchain technology compared to the traditional system.

4.1 Hardware Configuration

The hardware infrastructure design of this system is to be lightweight, powerful enough to perform complex cryptographic computations and process biometric

information. One key consideration is to ensure a storage capacity of no less than 40 GB, which is sufficient to hold the operating system, development kit, and local blockchain information. Secondly, for storing volatile memory, no less than 512 MB of RAM is required to run Python scripts smoothly along with smart contract interface functionality.

Besides the above basic computing specifications, the hardware configuration consists of specialized IoT-based Electronic Voting Machines (EVMs). The machines have highly advanced finger scanners for the purpose of capturing biometric information for Aadhaar authentication. The IoT technology enables the machines to have permanent connectivity to the cloud server and the blockchain network to enable instantaneous transmission of voting information without the use of manual data transfer.

4.2 Software Configuration

The software platform offers a conceptual foundation ideal for the process of decentralization and vote identity verification. The software project is developed on the Windows 7 operating system, acting as the host for the software development tools and networks. The coding process uses the Python coding language for its dynamic nature in handling IoT streams and advanced biometric analysis and communication capabilities.

4.3 Blockchain Migration

In the experimental setup, the first step involves migrating the blockchain network using the RunBlockchain file available in the *bin* folder of the blockchain framework. This process initializes the blockchain environment by executing the predefined network configurations and starting the required blockchain services. Upon execution, the system creates the genesis block and deploys the necessary blocks and smart contracts onto the distributed ledger. The migration ensures proper synchronization of data across all participating nodes and confirms successful initialization through system logs. This step establishes a secure and stable blockchain environment, which is essential for performing subsequent experimental operations and evaluations.

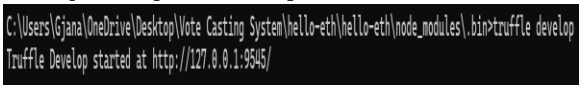


Figure.3 Running the server

The blockchain is migrated by executing the RunBlockchain file in the same command-line interface (CMD) from the *bin* folder.During migration, the smart contract is deployed and the contract address 0xD81b593289614721fFC85f7AE43B41dE2b3c736D is generated in the CMD output.This address is copied for further interaction with the deployed contract in subsequent experiments.

Figure.4 Hashkey generating

After copying the generated contract address, it is pasted into the view.py file.The contract address is configured within the application logic to enable interaction with the deployed smart contract.

This integration allows the system to perform blockchain operations such as data retrieval and transaction execution during experimentation.

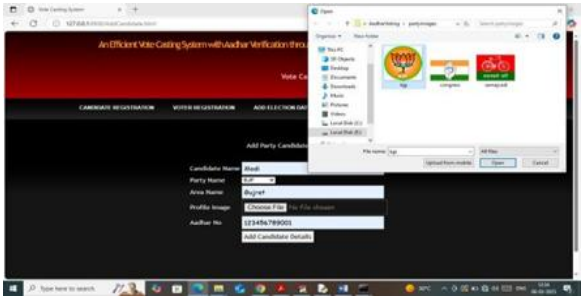
An Efficient Vote Casting System with Aadhar Verification through Blockchain\VotingApp After configuring the contract address in the view.py file, the manage.py file is executed to start the application server.This step establishes communication between the web application and the deployed blockchain smart contract.Successful execution confirms that the system is ready for blockchain-based operations and experimental evaluation.

The below figures 4(a)-4(h) explain the process to cost the vote.

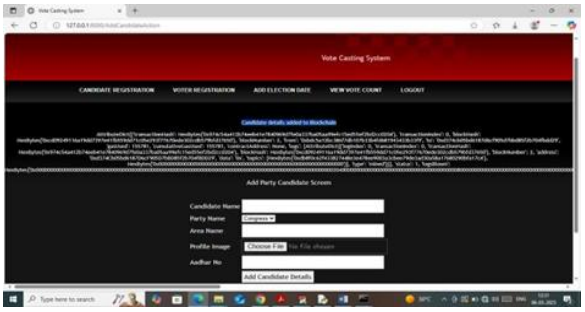
In above screen click on ‘Admin Login’ link to get below page

In above screen admin is login and after login will get below page

In above screen admin can click on 'Candidate Registration' link to add candidate details

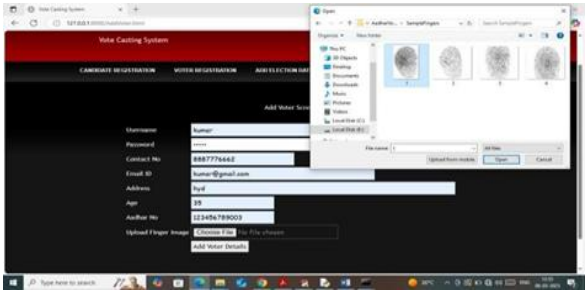


In above screen add candidate details along with party symbols and then press button to get below page



In above screen candidate details added to Blockchain and then in am displaying entire log obtained from Blockchain after data storage. In above log can see details like Transaction no, Block no, block hashcode and many other details. Similarly, you can add as many candidates as you want

In above screen adding another candidate and now click on 'Voter Registration' link to get below page



In above screen adding voter details along with Aadhar no and fingerprint and then press button to get below page. (Note we don't have Aadhar database or fingerprint scanner so we are uploading as image).

In above screen selecting and adding election date. You can choose any date but today only we have to run all modules so select today date only so voter can login and cast votes. Now click on 'View Vote Count' link to get below page

In above screen in blue text can see Voter votes successfully casted to selected candidate. Now click on 'Latency Graph' link to get below page

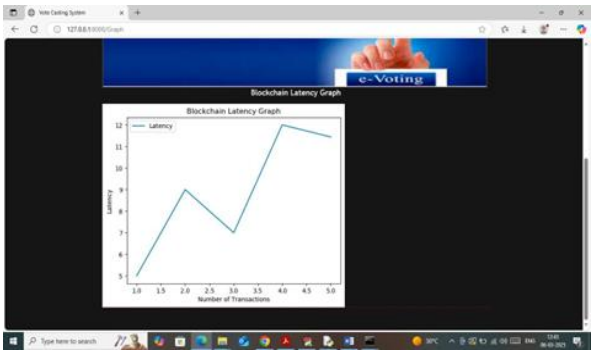


Figure.5 Performance of model

V. CONCLUSION

The proposed e-voting system adequately bridges the critical security and transparency gaps in traditional electoral processes through the integration of blockchain technology and Aadhaar-based biometric authentication. The Ethereum-based blockchain ensures that every vote is recorded as a tamper-proof transaction by utilizing its decentralized and immutable nature, thereby eliminating risks associated with centralized database manipulation and internal fraud. Its inclusion of fingerprint verification adds a robust layer to identify voters without allowing proxy voting and impersonation of voters, while voter anonymity is ensured through cryptographic hashing. Experimental results confirm that this hybrid IoT-Blockchain framework enables not only enhancement in the integrity and auditability of the democratic process but also streamlining of election administration with real-time tallying and automated smart contract execution.

REFERENCES

[1] Sah, A., Kumar, A., & Bhushan, B. (2025). "Leveraging Blockchain Technology for Secure Online Voting Systems: A Comprehensive Review." Journal of Mobile Multimedia, 21(3-4), 535–554. [DOI: 10.13052/jmm1550-4646.213412].

[2] Yao, J., Yang, B., Wang, T., et al. (2024). "A Distributed Self-Tallying Electronic Voting System Using the Smart Contract." Chinese Journal of Electronics, 33(4), 1063–1076. [DOI: 10.23919/cje.2023.00].

[3] Jacob, S. S., Varghese, L. J., et al. (2024). "Intelligent Data Storage in Electronic Voting Machine Using Blockchain System." IEEE Conference on Smart Technologies (ICSTSN), 1–5. [DOI: 10.1109/icstsn61422.2024.10670942].

[4] Patil, H. V., et al. (2024). "E-Voting System Using Blockchain." International Journal for Research in Applied Science & Engineering Technology (IJRASET), 12(III). [DOI: 10.22214/ijraset.2024.59313].

[5] Shwetha, R., et al. (2025). Fraud-Resistant Voting Using Aadhaar Authentication. International Journal for Multidisciplinary Research (IJFMR), 7(6).

[6] Paudel, P. (2025). Enhancing Electoral Integrity and Accessibility: A Blockchain and Facial Recognition-Based Electronic Voting System. Information Dynamics and Applications, 4, 85–94.

[7] Srilatha et al., 2024. Fingerprint-based biometric smart electronic voting machine using IoT and advanced interdisciplinary approaches. E3S Web of Conferences, 507, 01037. [DOI: 10.1051/e3sconf/202450701037].

[8] George, S. M., et al. (2024). "Aadhar Card Based Efficient Biometric Voting System." International Journal of Creative Research Thoughts (IJCRT).

[9] Satla, S., Shieh, C.S. (2025). Multi-model Telugu speech recognition: Improving ASR with dialect classification and optimization techniques. Traitement du Signal, Vol. 42, No. 6, pp. 3159-3169. https://doi.org/10.18280/ts.420611

[10] Kittu, V. (2024). "Meta-analysis of blockchain-powered electronic voting systems." MATEC Web of Conferences, 392, 01076. [DOI:10.1051/matecconf/202439201076].

[11] Almeida, R. L., et al. (2023). "Impact of decentralization on electronic voting systems: A systematic literature survey." IEEE Access 11, 132389–132423.