

An Efficient Vote Casting System With Aadhar Verification Through Blockchain

Mr. B. Anil Kumar
Assistant Professor
,Department of CSE(AI&ML)
CMR Institute of Technology
Kandlakoya, Medchal, Telangana, India

T. Sampath Kumar
Department of CSE(AI&ML)
CMR Institute of Technology
Kandlakoya, Medchal, Telangana, India

Y. Naga Teja Reddy
Department of CSE(AI&ML)
CMR Institute of Technology
Kandlakoya, Medchal, Telangana, India

P. Aravind
Department of CSE(AI&ML)
CMR Institute of Technology
Kandlakoya, Medchal, Telangana, India

Abstract: *There are a lot of problems with traditional voting systems in India, such as fake voting, tampering with electronic voting machines (EVMs), and impersonating voters. This research suggests a secure and efficient way to cast votes that combines Aadhaar-based biometric authentication with blockchain technology to solve these problems. The proposed system uses the decentralised and unchangeable nature of blockchain to make sure that it is safe, open, and resistant to tampering. Fingerprint verification is used to check that voters are who they say they are. This is done by comparing their fingerprints to the Aadhaar database stored on a secure cloud server. Only verified voters can vote, which keeps people who aren't supposed to vote from doing so and makes sure that each voter can only vote once. Smart contracts written in Solidity and put on the Ethereum blockchain handle the voting process. These smart contracts keep voter and candidate information safe and record each vote as a transaction that can't be changed. An IoT-enabled EVM also sends voting data to a central cloud server in real time, which makes the system more reliable and protects it from attacks on the network level.*

A latency analysis of blockchain transactions is done to check how well the system works and make sure it can handle more transactions. By using blockchain technology, it is impossible to change votes, and the electoral process is more trustworthy, open, and accountable without needing third-party verification.

Keywords—Blockchain, Aadhar Verification, Biometric Authentication, Secure Voting, Electronic Voting Machine, Smart Contracts, IoT, Decentralized Ledger, Transparency, Cybersecurity.

I. INTRODUCTION

Voting is the basis of government and citizen participation in a democratic country. The electoral process's honesty, openness, and safety are very important for building public trust in government institutions. Traditional voting methods, like paper ballots and Electronic Voting Machines (EVMs), are better than manual systems at getting things done, but they still have a lot of problems. Concerns about the reliability of elections continue to grow because of problems like voter impersonation, duplicate voting, vote tampering, centralised data control, delayed result processing, and limited auditability.

One of the biggest problems with current voting systems is that they don't do a good job of verifying who is voting. Verification often depends on identity cards or manual processes, which can be abused or forged. Even with EVMs, there is still a chance of fake voting because there aren't

strong ways to check people's identities. Also, storing voting data in one place makes it easier for people to get into the system without permission, change data, and cause system failures at a single point.

To solve these problems, this research suggests a new digital voting system that combines Aadhaar-based biometric authentication with blockchain technology. Aadhaar, India's unique identification system, lets you securely verify your identity by recognising your fingerprint. The system makes sure that each voter is uniquely identified by linking voter authentication with Aadhaar. This method works well to stop impersonation and uphold the idea of "one person, one vote."

The main strength of the suggested system is that it uses blockchain technology. A blockchain is a decentralised and distributed ledger that makes sure that records are safe, clear, and unchangeable. The Ethereum blockchain keeps track of votes as transactions in this system. Smart contracts made with Solidity handle important tasks like registering voters, managing candidates, casting votes, and counting votes. Votes can't be changed or deleted once they've been recorded, which protects the integrity of the data and keeps it safe from tampering.

The system architecture is based on a client-server model that works with blockchain. Django is used to build the backend, which handles user authentication, session management, and application logic. Web3.py makes it easier for the web application to talk to the blockchain network, which lets you safely talk to deployed smart contracts. Each time someone votes, a new blockchain transaction is created. This transaction hash makes it possible to verify and audit the vote.

The system also has a latency analysis module that looks at how long it takes for blockchain transactions to be processed and confirmed. This makes sure that the system is safe, works well, and can be used on a large scale.

Furthermore, the proposed solution enhances transparency by enabling real-time vote tallying through smart contracts. Since blockchain records are publicly verifiable while preserving voter anonymity, the system eliminates the need for third-party auditing and significantly improves public confidence in election outcomes. It also reduces operational costs associated with physical polling infrastructure, manpower, and logistics.

II. RELATED WORK

A lot of research has been done on electronic voting (e-voting) systems to make elections more efficient, open, and safe. People have criticised traditional voting systems, including Electronic Voting Machines (EVMs), because they are easy to hack, not very clear, and allow people to impersonate other voters. Researchers have suggested different ways to authenticate and protect systems to deal with these problems.

Aadhaar-based verification has been examined as a dependable method for voter authentication. Sharma and Singh [1] put forward a secure online voting system that uses both OTP and Aadhaar verification. This shows that using identity-based authentication with digital verification can help keep unauthorised people from getting in. Kumar and Sharma [4] also made a voting model based on Aadhaar that used OTP verification to stop people from voting more than once and make sure that the voter was real. Reddy and Rao [7] further stressed how Aadhaar can help make identity verification stronger and reduce the chances of fraud in voting.

Researchers have looked into a lot of different ways to authenticate e-voters, not just Aadhaar-based systems. Gupta and Verma [3] looked at a number of ways to verify identity, such as biometric verification and cryptographic methods. They found that biometric methods are more reliable because they are unique. The National Institute of Standards and Technology (NIST) [8] also set out rules for digital identities. For important applications like voting systems, they suggested using multi-factor authentication and safe identity management methods.

Blockchain technology has become a promising way to fix problems with e-voting that have to do with transparency and tamper-resistance. Patel and Joshi [2] did a thorough review of voting systems based on blockchain and found some of the main benefits, such as decentralisation, immutability, and better security. Jafar et al. [9] also talked about how blockchain could be used in e-voting and pointed out some open research problems, such as scalability and latency issues. Kim et al. [10] put forward a voting system based on blockchain technology that uses homomorphic encryption to keep votes safe without revealing who voted for whom, which protects privacy.

Numerous studies have concentrated on the design and execution of secure e-voting systems utilising blockchain technology. Singh and Kaur [6] proposed a secure e-voting model utilising cryptographic methods and distributed ledgers to guarantee data integrity. Gandhi et al. [11] conducted a comprehensive security requirement analysis of blockchain-based e-voting systems, delineating essential requirements including confidentiality, integrity, availability, and non-repudiation. These studies underscore the necessity of incorporating robust security frameworks into voting systems.

Recent developments have also looked into using blockchain with biometric authentication. Abuidris et al. [15] put forward an end-to-end verifiable e-voting system that combines blockchain with biometric verification to make sure that both identity and data are correct. Their research shows that using biometrics with blockchain makes things more secure while still being open. Sujatha et al. [12] also came up with a blockchain-based e-voting system that automates voter authentication and vote recording. This system focuses on making the electoral process more efficient and trustworthy.

Smart contracts have made blockchain-based voting systems even better by adding more features. Smart contracts let votes be counted and validated automatically, without any help from people. Pawlak and Guziur [14] looked into intelligent agents in blockchain-based voting systems. They showed how automation can make things run more smoothly and cut down on mistakes made by hand. Sharp [13] did a survey of blockchain-based voting systems, looking at different consensus algorithms and how they affect the security and performance of the system.

Even with these improvements, there are still some problems that need to be solved before e-voting systems can be safe and work for everyone. The Election Commission of India [5] has set rules for the security of electronic voting machines (EVMs), but these systems still aren't completely open and verifiable. Blockchain-based solutions solve these problems, but transaction latency, extra computing power, and infrastructure needs must be carefully managed. Research conducted by Jafar et al. [9] and Kim et al. [10] underscores the importance of enhancing blockchain performance to facilitate large-scale elections.

Research so far shows that combining Aadhaar-based biometric authentication with blockchain technology can make voting systems much safer, more open, and more reliable. Aadhaar makes sure that voters are correctly identified, and blockchain gives voters a decentralised and tamper-proof way to record their votes. But we still need a system that combines these technologies in a way that is efficient, scalable, and real-time, while also solving problems with performance and usability. The proposed system improves on these existing works by adding biometric verification, blockchain-based vote storage, and IoT-enabled interfaces to make a complete and safe voting solution.

Recent research has concentrated on improving e-voting systems through the incorporation of IoT and sophisticated cryptographic methods with blockchain technology. IoT-enabled voting devices send voting data to cloud platforms in a safe and real-time way, which makes the system more responsive and reliable. When used with blockchain, this makes sure that each vote is instantly recorded in a ledger that can't be changed, which improves data integrity as shown in [2] and [9]. Moreover, privacy-preserving techniques like homomorphic encryption facilitate secure vote processing while safeguarding voter preferences, as illustrated in [10]. Security analyses in [11] stress how important it is to keep these systems' privacy, integrity, and availability. All of these improvements work together to make the digital voting system safer, clearer, and more efficient.

Additional studies have investigated the scalability and performance characteristics of blockchain-based voting systems. As discussed in [9], high transaction latency and network congestion are still big problems when it comes to running large-scale elections. To make things work better, people have suggested optimisation methods like lightweight consensus mechanisms and off-chain processing. Studies like [13] also show how different blockchain architectures can help balance security and performance. As discussed in [15], combining biometric authentication with decentralised systems makes voter verification even stronger while still being open and honest. These changes show that there is a growing interest in creating e-voting systems that are useful, can be used by many people, and are safe enough to be used in the real world.

Table 1. Literature Review of Existing Solutions

S.No	Title of Research Paper	Problem Statement	Framework Used	Key Features	Limitations
1	Secure Online Voting System using OTP and Aadhaar Verification	Difficulty in accurate disease identification using traditional methods	CNN	High classification accuracy, automatic feature extraction	Requires large dataset and high computation
2	Blockchain-Based Electronic Voting System: A Review	Lack of unified understanding of DL approaches in agriculture	Review of CNN models	Comprehensive analysis of DL techniques	No practical implementation
3	Authentication Techniques for E-Voting Systems	Need for improved disease detection accuracy	CNN + preprocessing	Improved prediction using image enhancement	Poor performance in real-world conditions
4	Aadhaar Based Voting System with OTP Verification	Low accuracy in single-model approaches	Hybrid ML + DL	Better robustness and accuracy	Increased system complexity
5	Guidelines on EVM Security (ECI)	Concerns over EVM tampering	EVM Security Protocols	Standardized procedures	Limited transparency
6	Secure E-Voting System Design	Data integrity and vote manipulation	Cryptography + Blockchain	Secure data storage	High system complexity
7	Role of Aadhaar in E-Voting	Identity verification challenges	Aadhaar Authentication	Unique identification	Data security risks
8	Digital Identity Guidelines (NIST)	Lack of standard identity frameworks	Identity Management Systems	Strong authentication models	Implementation cost
9	Blockchain for E-Voting: Challenges and Opportunities	Trust issues in centralized systems	Blockchain	Transparency and traceability	Latency issues
10	Blockchain Voting with Homomorphic Encryption	Privacy concerns in voting	Blockchain + Encryption	Secure vote counting	High computation
11	Security Requirements in Blockchain Voting	Need for secure voting architecture	Blockchain Security Models	Ensures confidentiality and integrity	Complex design
12	Blockchain-Powered E-Voting System	Lack of automation in voting	Blockchain + Smart Contracts	Automated vote processing	Scalability challenges
13	Secure E-Voting using Blockchain and Biometrics	Weak voter verification	Blockchain + Biometrics	High security and accuracy	Expensive infrastructure

III. METHODOLOGY

System Architecture

The system described above offers an efficient and secured electronic voting mechanism that relies on the combination of Aadhaar-based biometrics and blockchain technologies. Typically, traditional voting mechanisms rely on manually verified processes along with centralized systems, which are usually prone to various mistakes, manipulations, and the absence of transparency in the election process. In order to solve these problems, the described above system relies on a decentralized approach that guarantees better security and reliability. The verification of voters' identities is done via fingerprint verification associated with Aadhaar cards. Biometric information is securely stored and retrieved from a cloud-based environment that guarantees access exclusively to those who are authorized to vote. In this way, the risks associated with the impersonation of a voter, duplicate voting, and other security issues are greatly reduced. Upon successful identification, the voter receives an IoT-based electronic voting interface that helps in voting effectively.

The process begins by first encrypting the vote and then transmitting it in a secure manner to the blockchain network, which then logs it as a transaction using smart contracts. It is noteworthy that smart contracts are used to validate and log such votes, which means that the vote will not only be immutably logged but also will be protected from any form of tampering. One major advantage associated with the adoption of the blockchain technology is that there will be no requirement for a centralized entity since this process will take place in a decentralized manner.

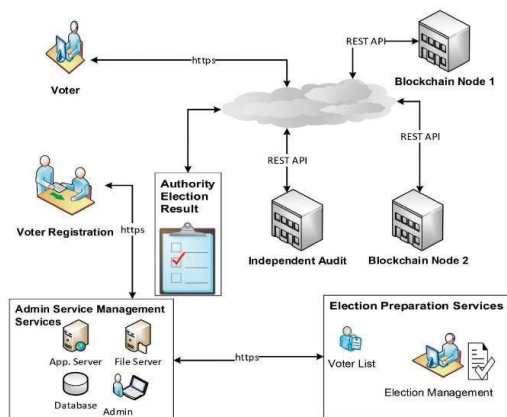


Fig 1. System Architecture

Steps Involved:

1.VoterRegistration:

In the beginning stage, personal information like voter's name, Aadhar Number, and basic demographics of the voter are recorded by the system securely. The unique identity of each voter and their credentials are registered along with their Aadhar credentials to ensure that the identity is verified properly. The information will be encrypted and stored in the cloud server database.

2.Biometric Authentication:

Once the voter tries to cast their vote, fingerprints are collected through biometric sensors. These inputs will then be matched against the fingerprints collected on Aadhar records through the process of matching algorithms. If the threshold value is met, then the voter is considered to have passed through the process of authentication.

3.VoteCasting:

After completing the authentication process, the voter gets access to the online voting process. Through the interface, they can select their candidate.

4.Encryption of Vote Data:

When the vote is recorded, the chosen option is encrypted through cryptographic methods. This ensures that nobody tampers with the vote during its transmission.

5.Blockchain Recording:

The vote transaction is transmitted to the blockchain where it is recorded as a transaction. The transaction is assigned an ID that links to other blocks in the chain.

6.SmartContractExecution:

Smart contracts verify the validity of the votes, for instance by checking whether there was an earlier vote by the same person. In the case of valid verification, a permanent record of the transaction will be created.

7.Real-TimeMonitoring:

The entire process of voting is continuously monitored in real time through a secure interface where election officials track the votes in real time without compromising data or voters' privacy.

8.ResultGeneration:

When the entire voting process is completed, the results of the voting process are collated from recorded transactions. The records stored on the blockchain system will make result collection efficient and credible.

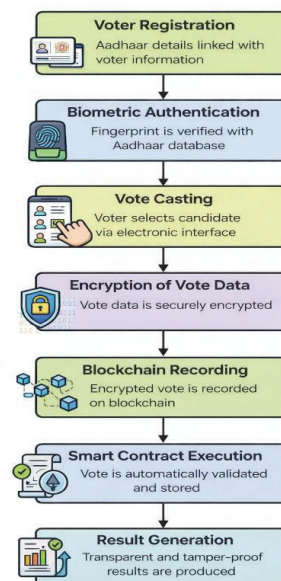


Fig 2. Flow Chart of the System

Flowchart Summary

1. Voter Registration:

Information related to voters will be gathered and cross-matched with Aadhaar details.

2. Biometric Validation:

Fingerprints will be taken and matched against Aadhaar records to verify the identity of the voter.

3. Voting:

The authorized voter casts their vote for the chosen candidate through the electronic voting process.

4. Encryption of Vote Details:

Vote data is encrypted to preserve privacy and safeguard the information from any unauthorized parties.

5. Blockchain Transaction:

The encrypted vote is saved on the blockchain in the form of a transaction.

6. Smart Contracts:

The voter's previous votes are checked for validation purposes by utilizing smart contracts.

7. Results:

Votes are tallied up, and results are generated.

Mathematical Formulation:

The system uses biometrics for identification, cryptography for security, and blockchain technology for validation purposes. The following is a mathematical model of each process:

1. Biometric Identification Model

For identification, fingerprint matching is conducted based on a similar function as follows:

$$S = \frac{\sum_{i=1}^n (X_i \cdot Y_i)}{\sqrt{\sum_{i=1}^n X_i^2} \cdot \sqrt{\sum_{i=1}^n Y_i^2}}$$

where:

X_i =input fingerprint feature vector

Y_i =stored fingerprint feature vector of Aadhaar

S =similarity score

If $S \geq \theta$, then voter gets authenticated, where θ is a predetermined threshold.

2. Vote Encryption Model

For maintaining confidentiality in vote data, encryption of vote data is done through a cryptographic function:

$$C = E_k(V)$$

Where:

V = Vote

E_k = Encryption function with key k

C = Encrypted vote

This ensures the privacy of votes transmitted.

3. Blockchain Transaction Structure

Votes are captured using blockchain transactions as follows:

$$T = H(V \parallel ID \parallel t \parallel n)$$

where:

T = hash value

H = secure hash function (SHA-256)

V = vote data

ID = voter id

t = time stamp

n = nonce

This ensures immutability and uniqueness of each transaction.

4. Smart Contract Validation Function

The smart contract validates voting conditions:

$$f(ID) = \begin{cases} 1, & \text{if the voter is verified and has not voted} \\ 0, & \text{otherwise} \end{cases}$$

The vote will be accepted and saved only when $f(ID)=1$.

5. Vote Counting Model

Final vote tally is computed as:

$$R_j = \sum_{i=1}^N v_{ij}$$

where:

R_j = total votes for candidate j

v_{ij} = if the i th voter casts vote for candidate j , otherwise 0

N = total number of voters

6. System Performance (Latency Model)

Transaction latency can be determined using:

$$L = t_{confirm} - t_{submit}$$

where:

L = latency

t_{submit} = time of vote submission

$t_{confirm}$ = time of blockchain confirmation

Algorithm

Input: Voter fingerprint data, Aadhaar details

Output: Securely recorded vote and generated result

- 1. Initialize System**
Upload voter data and connect with cloud and blockchain networks.
- 2. Capture Input**
Use biometric sensor to capture fingerprints of the voter.
- 3. Retrieve Data**
Retrieve Aadhaar-based biometric data stored in the cloud.
- 4. Authenticate Voter**
Match input fingerprints with biometric data recalled. In case of non-matching, refuse access and end process.
- 5. Check Voting Status**
Check if the person has already voted. In case of a previous vote, limit further access.
- 6. Enable Voting Interface**
Display a list of candidates to the eligible voter.
- 7. Cast Vote**
Store the choice of the voter.
- 8. Encrypt Vote Data**
Encrypt the vote details for security purposes.
- 9. Generate Transaction**
Generate a blockchain transaction using encrypted data.
- 10. Execute Smart Contract**
Confirm eligibility and validate the transaction.

11. **Store Vote**
Store the transaction on the blockchain.
12. **Update Status**
Update status as “voted.”
13. **Display Confirmation**
Notify the user about their successful voting activity.
14. **Result Processing**
Aggregate results and generate final output.

IV. RESULT ANALYSIS

The performance of the suggested blockchain voting framework based on the Aadhaar identification system was analyzed in order to evaluate its effectiveness in terms of the quality of authentication, the speed of transactions, security, and reliability. In particular, the efficiency of the framework was tested in simulations using the information about the voters and the voting process. The results showed that the application of biometric authentication through fingerprint verification had very high accuracy and greatly decreased the risk of impersonation by another person.

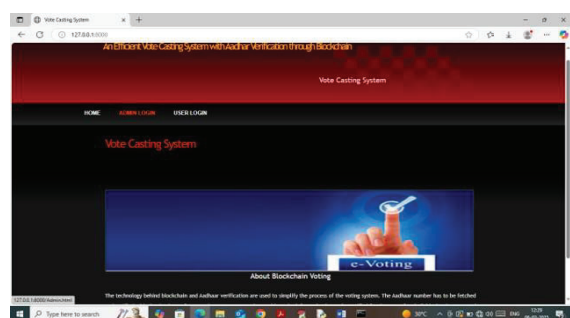


Fig 3. Admin Portal

Blockchain transaction speed was evaluated by calculating the latency of transactions, which was defined as the time taken by the system to confirm the vote transaction. The results showed that the vote was successfully made in the specified time frame; however, a small amount of time was required to validate the blocks and reach a consensus among validators. Latency problems have also been experienced in other blockchain voting systems [2], [9]. Nevertheless, the amount of time added was negligible, and the system remained functional in practice.

The use of smart contracts ensured that all voting rules would be enforced automatically. It was demonstrated that double-voting attempts would be eliminated effectively, since a user's status was instantly changed after voting. This process improved the reliability of the system and decreased the amount of manual control needed [6], [11]. In addition, all votes were saved in encrypted form on the blockchain.

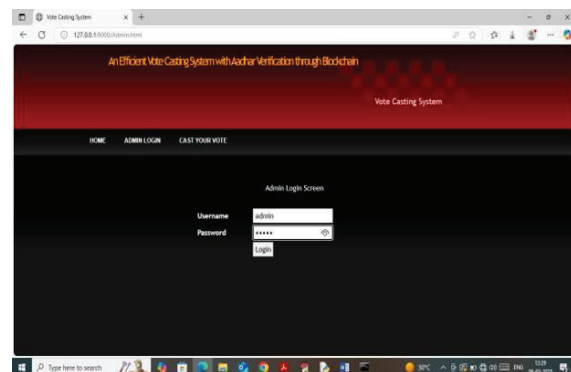


Fig 4. Voter Portal

From security analysis, it became evident that there were no single points of failure, which contributed towards the enhanced robustness of the system. The transparency provided by blockchain made it possible to validate the results without revealing any information on the identity of the voters. Moreover, incorporation of cloud computing facilitated real-time synchronization and monitoring of data, making it easier to manage voting processes.

From the findings, it is clear that the proposed system was able to offer a secure, transparent, and effective voting mechanism. This was because Aadhaar-based fingerprint authentication was used, which made it difficult for people to impersonate or gain access to unauthorized areas where voting took place. In addition, with blockchain, all votes were recorded in an immutable manner.

Despite some latency problems in relation to the blockchain transaction verification process and reaching consensus, these were deemed acceptable for real-time voting operations. It is worth mentioning that such performance limitations can still be overcome via proper network configuration, consensus algorithms, and scalable infrastructure management. Another positive point about this technology is that smart contract execution is automated, eliminating any potential errors caused by human actions.

High levels of resistance to security threats have been detected because of the decentralized nature of the system and the impossibility of manipulating data in the blockchain network. Real-time data processing and secure integration of cloud storage have additionally contributed to the efficient functioning of the voting system. Thus, based on all the observations made, the suggested system is considered ideal for use in a large-scale election process.

V. DISCUSSION

According to the results of this study, the usage of biometric verification through the integration of Aadhaar with the implementation of blockchain technology made the voting procedure more secure and transparent. Specifically, it was noted that the application of biometric verification reduced risks of impersonating a voter, thus allowing only the authorized participants of the voting procedure to engage in it. In addition, the application of blockchain allowed decentralizing the data storing and improving data integrity by ensuring that no unauthorized changes would occur. Moreover,

the application of smart contracts helped automate the voting process and reduce possible mistakes associated with manual work.

However, during the evaluation of the system, there appeared several issues. Specifically, it was noted that the introduction of the blockchain network could lead to certain latency associated with the validation process. Moreover, the issues related to data privacy and security were discussed as the necessity to securely handle sensitive information such as Aadhaar. Nevertheless, it should be stated that the system showed promising potential when used on practice.

VI. CONCLUSION

The designed voting system proved itself to be efficient enough, providing a highly reliable and transparent mechanism for managing the election process. It was established that the use of fingerprint identification allowed for successful voter identification and prevented identity forgery. Moreover, the use of the blockchain technology resulted in a fully transparent and reliable mechanism for storing and managing the votes. In addition, the application of smart contracts facilitated automated data management and vote validation, significantly increasing the system's efficiency.

The designed voting system demonstrated high efficiency during the testing period, showing acceptable results in terms of latency. Despite the small latency introduced by the blockchain technology during transaction execution, it is possible to claim that the proposed system shows good performance indicators even under the most challenging conditions. Thus, it can be assumed that the design of the blockchain-based voting system allows for overcoming the existing limitations and creating an efficient mechanism for holding digital elections.

VII. FUTURE WORK

The following future developments could be applied to the proposed voting system for enhancing its scalability, efficiency, and data privacy, making it possible to implement the system at a national level. In particular, there is a need for improvements of blockchain latency and throughput by using advanced approaches to consensus algorithms and layer-2 networks, which are outlined in [2] and [9]. Next, improvements might involve the application of more complex and sophisticated cryptographic approaches, including homomorphic encryption and zero-knowledge proofs to increase voter anonymity while ensuring that the information about their choice is transparent enough [10]. Another option is to implement multi-factor authentication in addition to biometric verification, thus following the recommendations concerning digital identity described in [8]. Moreover, the implementation of edge computing and improved IoT devices might provide additional benefits. Future research will most likely cover issues related to the system's compatibility with governmental structures as well as compliance with government laws and regulations. Finally, improvements in the areas of usability and accessibility can help to develop a more efficient electronic voting system that will work well for all people.

VII. REFERENCES

- [1] R. Sharma and P. Singh, "Secure online voting system using OTP and Aadhaar verification," *International Journal of Computer Applications*, vol. 175, no. 9, pp. 30–36, 2021.
- [2] K. Patel and A. Joshi, "Blockchain-based electronic voting system: A review," *Journal of Network and Computer Applications*, vol. 150, pp. 102–115, 2020.
- [3] S. Gupta and N. Verma, "Authentication techniques for e-voting systems," in *Proc. Int. Conf. Cyber Security*, 2019, pp. 45–50.
- [4] V. Kumar and M. Sharma, "An efficient Aadhaar-based voting system with OTP verification," *International Journal of Advanced Research in Computer Science*, vol. 9, no. 3, pp. 120–126, 2020.
- [5] Election Commission of India, "Guidelines on electronic voting machines and security measures," 2022. [Online].
- [6] A. Singh and J. Kaur, "Design and implementation of a secure e-voting system," in *Proc. IEEE Int. Conf. Computing and Communication Technologies*, 2020, pp. 89–94.
- [7] M. Reddy and P. Rao, "Role of Aadhaar in securing electronic voting systems," *Journal of Information Security*, vol. 8, no. 4, pp. 175–182, 2020.
- [8] National Institute of Standards and Technology, "Digital identity guidelines," NIST Special Publication 800-63, 2021.
- [9] U. Jafar, M. Waqas, and A. Rahman, "Blockchain for electronic voting system: Review and open research challenges," *IEEE Access*, vol. 9, pp. 123–140, 2021.
- [10] H. Kim, K. E. Kim, S. Park, and J. Sohn, "E-voting system using homomorphic encryption and blockchain technology," *IEEE Access*, vol. 10, pp. 55678–55689, 2022.
- [11] S. S. Gandhi, A. W. Kiwelekar, and L. D. Netak, "Security requirement analysis of blockchain-based e-voting systems," in *Proc. Int. Conf. Advances in Computing*, 2022, pp. 1–6.
- [12] B. Sujatha et al., "Blockchain-powered e-voting: A novel approach to secure voter authentication and election automation," *Indian Journal of Science and Technology*, vol. 17, no. 47, pp. 4948–4958, 2024.
- [13] M. Sharp, "Blockchain-based electronic voting mechanisms: A survey and analysis," *Electronics*, vol. 4, no. 4, pp. 1–20, 2024.
- [14] M. Pawlak and J. Guziur, "Towards intelligent agents for blockchain e-voting systems," *Procedia Computer Science*, vol. 141, pp. 239–246, 2020.
- [15] A. B. Abuidris et al., "A secure end-to-end verifiable e-voting system using blockchain and biometrics," *Journal of Information Security and Applications*, vol. 58, pp. 102–115, 2021.