International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

A Decentralized and Biometrically Secured E-Voting Framework using Hybrid Encryption

Nausheen Nahid, Rajarajeswari P, Tamilarasi C

Student, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India

Student, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India

Professor, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT : Electronic voting systems have been given more attention and popularity due to the potential of improving efficiency and availability of the voting process, nevertheless, the systems have continued to bring in various challenges in terms of security, transparency, athenticity of the voters and trust. The traditional central electronic voting systems have various disadvantages including data manipulation, single point failure, unauthorized access, etc. To eliminate the setbacks that were encountered by the traditional electronic voting systems, a new electronic voting system is introduced, which is termed as BLOCKVOTE. The new electronic voting system employs the principle of biometric authentication to authenticate the voter with the assistance of the blockchain concept and the concept of hybrid encryption based on the Advanced Encryption Standard (AES) to encrypt the vote data and the use of Rivest-Shamir-Adleman (RSA) to authenticate the voters. The new electronic voting system also makes use of the notion of Content Identifier (CID) and InterPlanetary File System (IPFS) where the vote data is stored. The voting process, voter registration, casting, validation, and computing of the results, are handled by smart contracts and therefore, the voting process is automated and no human intervention is required at all. The architecture of the system makes the process verifiable, anonymous and resistant to common cyber attacks that may affect the integrity of the electoral process, including vote tampering, impersonation, and replay attacks. Out of the experiments, BLOCKVOTE is capable of the secure, transparent, and scalable management of the electoral process with a minimum latency, which is why it can be considered as part of the new outlook of digital democracy.

KEYWORDS: Blockchain, Electronic Voting System, Biometric Authentication, Hybrid Encryption, AES, RSA, IPFS, CID, Smart Contracts, Decentralized Security

I. INTRODUCTION

Electronic voting has emerged as one of the possible solutions to the problem of efficiency, availability, and speed in the context of the contemporary democracy processes. Electronic voting systems are replacing the traditional voting systems due to the heightened use of electronic system in governance. In spite of the benefits of electronic voting systems, the systems continue to experience several challenges such as security, transparency and trust. Centralized electronic voting systems are so insecure and open to cyber attacks, manipulations, and one point failure that can disrupt the outcome of the elections.

Besides the above, there is the problem of voter validation which is another significant issue in the way of electronic voting systems. The traditional systems of verification, including passwords, voter ID and PIN are usually prone to duplication and unauthorized access. In the electronic voting system, any vulnerability in terms of verifying voters can cause threat to the principle of one person one vote by creating a risk in the forgery, duplication and denial of service, and the centralization of the sensitive information to the voters and the election in the database has created a critical privacy issue of concern in the fact that any access to the information when not supposed to be accessed can lead to misuse of such information by malicious actors.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

In order to reduce the above problems, decentralization with the aid of blockchain technology has become a more and more popular choice of the means of taking secure voting systems. The blockchain technology provides an unreliable and transparent registry in the absence of a central authority of trust. Thus, systems that are based on blockchains can ensure the integrity and verifiability of votes. Nevertheless, effective data protection and voter authentication systems should be established to provide the blockchain-based systems with the ability to guarantee the efficiency and security of the voting process.

The following article presents a biometrically secure and decentralized architecture of electronic voting system that is labeled as BLOCKVOTE. This architecture is a combination of the blockchain technology and hybrid encryption. The biometric techniques guarantee the active involvement of the voters in the election process. In the meantime, the vote data is safely encrypted by the use of Advanced Encryption Standard (AES). On the same note, key exchanges and access controls are also being carried out using RSA encryption in order to achieve a secure operation. Moreover, to be more decentralized and efficient in terms of storage, the vote information is safely stored through InterPlanetary File System (IPFS) and Content Identifier (CID) addressing.

Under the framework proposed, the difference between secure voter authentication and decentralized and transparent vote management will be closed. This revolutionizes the existing electronic voting system into an extremely insecure and centralized system to a secure and decentralized digital voting system. BLOCKVOTE has been suggested in order to see the creation of a strong and safe voting process that can suit the requirement of the current voting procedures. This process ensures privacy and integrity of the voter and creates more voter confidence.

II. BACKGROUND AND MOTIVATION

Some of the stakeholders of the electronic voting system include verification bodies, authorities, voting system computation bodies, and voters. Development of trust among these parties is an issue that is rather complicated, particularly because of the centralized voting system that we have at the moment. In centralized voting system there is only one body that takes care of voter databases, storage of votes and computation of results. It is one of the greatest security threats, and because of this threat, it may be hard to develop trust among voters and the authorities to confirm the authenticity of the voting system.

The rationale behind this study is that there is a higher potential of fraud and cyber attacks that are being targeted at electronic voting systems. In centralized voting system when an unauthorized access is provided to a server then the votes can be altered, erased or modified without the officials knowing this. In a conventional system, authentication is not highly implemented and this can be impersonated, duplicate votes and theft of credentials. Moreover, people cannot rely on the voting system because they cannot check whether the votes are being cast, saved and calculated properly since there are no verifiable end-to-end voting records.

Security and confidentiality of the information regarding the election and the data of the voters is another important factor. The votes executed via a network or aggregated on a central database can be hacked and stolen. Furthermore, in the absence of the intensive cryptography systems, attackers can exploit the vulnerabilities to key management systems and data storage systems. This indicates that there is necessity to have a strong and transparent voting system, which has the capability of upholding integrity and confidentiality of votes.

To overcome the issues that come with the voting systems, the work suggests the solution with an integrated decentralized architecture through the assistance of biometric authentication systems, combined cryptographic systems and blockchain network. Biometric systems also guarantee the eligibility of the voters when they are voting. The confidentiality of votes is also under AES encryption. It is also the case that the work encrypts key exchange and access control systems with RSA encryption. An immutable vote ledger is also created by a permissioned blockchain network. Also, the work employs the IPFS network and the assistance of CID addressing to store the votes in a decentralized way, which bridges the divide between identity verification of voters and transparent digital governance, as a result, laying the groundwork of a secure, scalable, and resilient electronic voting system.

III. RELATED WORK

Electronic voting has received widespread research on the application of blockchain-based electronic voting systems to enhance the transparency, integrity, and trustworthiness of electronic voting. The manner in which the process of consensus can be enhanced in terms of decentralization and reliability has been examined by various scholars.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

Specifically, Misic et al. [1] suggested that a Qualified Proof of Stake (QPoS) approach should be used to enhance blockchain-based networks in terms of fairness and fault-tolerance. QPoS is dynamic in that the stake of the nodes is determined by their past history. This approach will increase the reliability of the consensus process, which is important to the scalability of the electronic voting system, but will not deal with the application-level issues.

To avoid voter impersonation and identity fraud, biometric authentication systems have been suggested. Alotaibi et al. suggested an algorithm to give direct cryptographic key pair derivation using biometric characteristics, which binds the identity of the voter closely to transactions in the blockchain. A technique of applying fingerprint authentication alongside AES-GCM encryption was suggested by Ramesh et al. to enhance the confidentiality and integrity of votes. Although enhancing the security of the voting system, these methods are founded on the partially decentralized architecture and fail to utilize the full potential of blockchain technology.

A number of scholars have suggested blockchain-enhanced voting systems over which voters are authenticated by a biometric technique to enhance the safety of the voting system. Sharma et al. suggested a voting system which is based on blockchain technology and thus the impartiality of votes is guaranteed by applying smart contracts to block the occurrence of multiple voting of a particular person or their votes during the election process. On the same note, Patel et al. developed a voting system based on blockchain technology that guarantees the inalterability of any vote with the help of smart contracts to avoid a case of double voting during the election process.

Nevertheless, they do not favor the hybrid encryption and storage which matters in the election.
Professional cryptographic methods have been employed by other scholars in order to endorse privacy and verifiability. Zhang et al. [6] relied on the blind signatures and zero-knowledge proofs to support the voter privacy and verifiability and Kapsoulis et al. [7] relied on linkable ring signatures to support voter privacy and remove the issue of double voting. These methods are effective, but not easy to apply because of the computing costs.

End-to-end verifiable and decentralized voting systems have been utilized by other researchers. The systems applied in [8] and [10] by Hassan et al. and Singh et al. were online voting systems that used encrypted ballots through blockchain. These are good voting systems but fail to give the option of voter authentication through biometric checks and hybrid encryption.

Future-proof voting systems have been employed by other researchers. Kim et al. [9] and Ahmed et al. [15] employed post-quantum cryptography and deep learning-based biometric to assist in future-proof voting
.
Although such systems have high security guarantees, they provide complexity and make the system deployment more expensive. Li et al. in their study [11] and Verma et al. in their study [12] designed hybrid and decentralized blockchain systems to enhance the scalability and performance of the systems. The systems however do not have multi-layered security like biometrics and hybrid encryption.

The homomorphic encryption system invented by Mehta et al. in their study [13] allows the secure vote tallying without the decryption of the specific votes. But the significant disadvantage of the system is that it is a computationally expensive one. In their study, Rao et al. [14] and Kaur et al. [16] came up with biometric authentication systems on the basis of blockchain-based encrypted ballots to enhance the security of the electoral system.

Summary of Research Gap:
Based on the literature scrutiny, it is apparent that though the transparency and immutability is guaranteed by the incorporation of blockchain and the voters are authenticated via the biometric tool, the majority of the available frameworks are confined to the individual security measures of the voting process. There are only a handful of frameworks that have been known to incorporate all of these security measures such as biometric authentication, hybrid encryption, decentralized control of the blockchain, and off-blockchain storage into one framework. Moreover, storage and scalability of encrypted votes are also a problem that should be solved.

To address the shortfalls of the current frameworks, a new framework (BLOCKVOTE) is suggested that employs a hybrid approach to encryption and blockchain with the assistance of IPFS and CID-based decentralized storage in order to implement a secure, scalable, and transparent electronic voting system.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

IV. PROPOSED WORK

This paper describes a biometrically secure e-voting system, which is decentralized and called BLOCKVOTE. The system has been created to address the security, transparency and trust factors that come with the current e-voting systems. BLOCKVOTE is created to destroy the central control and single points of failure by applying the blockchain technology. BLOCKVOTE is a developed web-based e-voting system, which is implemented with a permissioned Ethereum blockchain network.

BLOCKVOTE system is proposed on the basis of entities. The proposed BLOCKVOTE system has three entities, namely Election Committee, Candidates and Voters. All the entities have been appropriated with roles and access levels. The Election Committee is involved in the whole process of the election. Applicants will have to send their nominations to the suggested BLOCKVOTE system. The Election Committee verifies and approves such nominations prior to the process of the election. Only after undergoing a multi-layered authentication process, voters are given the opportunity to participate in the election process.

BLOCKVOTE secures itself with strong voter authentication systems in case impersonation and unauthorized voting are to be performed. These types of authentication systems guarantee that only the legitimate voters could take part in the voting process and that the principle of the one person-one vote is followed. To this end, BLOCKVOTE employs one-time password and biometric facial recognition using a one-time password authentication.

Vote confidentiality and integrity is guaranteed by the application of a hybrid encryption model. To this end, the votes are coded with advanced encryption standard (AES) in order to provide effective and secure data transmission. Moreover, the Rivest-Shamir-Adleman (RSA) public-key encryption is also used to encrypt the AES encryption key to make sure that the access to the encrypted vote is regulated and authorized throughout the tallying procedure. The smart contracts anonymize the encrypted votes and save them in the InterPlanetary File System (IPFS), and the corresponding CID is registered in the blockchain.
The blockchain, where smart contracts can be found, aids in the automation of essential election operations to include, but not be limited to, vote validation, the removal of any form of double voting, the verification of the votes, and calculation of the election outcomes. This makes human beings not to take part in vital procedures and gives the election exercise transparency and security.

Objectives of the Proposed System

- Develop a decentralized e-voting system, which offers tamper-resistant and immutable vote registration using blockchain.
- Impersonation and repeat voting should be eliminated by enforcing voter authentication based on multi-factor methods like OTP and facial recognition that is biometric-based.
- Secure and maintain integrity of vote information by using a hybrid encryption method that uses AES and RSA.
- To use IPFS-based decentralized storage to store encrypted vote data in a form, which can be used to enable voter anonymity and scalability of the system.
- To be used in automating election procedures to include vote validation, recording and calculation through smart contracts on blockchain.
- To allow transparent visualization and verifiable results computation.
- To provide a safe and effective online system to electoral bodies to handle voter registration, candidates, and the entire election systems.
- To enhance confidence in the electronic voting systems by use of safe and auditable election system.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

V. SYSTEM MODULES

The proposed blockvote system has been developed to be in the form of a modular structure to cater to scalability, security and proper management of the election process. The various modules in the proposed model will be tailored to complete certain functions and modules will be connected to one another by secure and well-defined interfaces to make the e-voting process transparent and tamper proof.

A. Voter Module

The suggested Voter Module is guaranteeing the registration, identification and casting of the votes to the voters. In the suggested model the registered voters will be taken through a multi-factor authentication system including OTP and facial recognition, to verify who the voter is. Once the identification process is completed, the voter is allowed to make one vote, encrypted, and anonymized and submitted to decentralized storage and blockchain recording. In the model suggested, the identity of the voter and ballot are maintained apart to guarantee the anonymity of the voter.

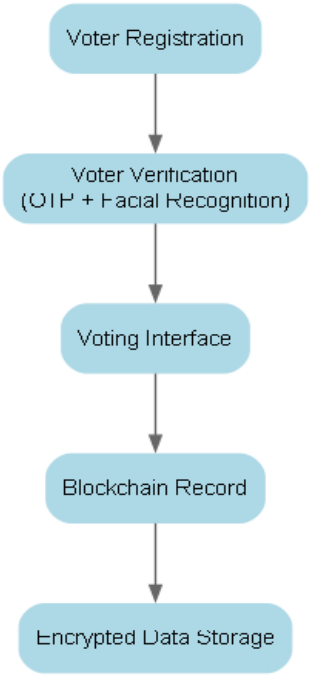

Fig 1 Voter Module

B. Candidate Module

The proposed Candidate Module guarantees the registration, nomination as well as the involvement of the candidates in the election. In the suggested model, nomination information is presented by the candidates into the system, and it is validated by the Election Commission. Once the verification is done, the candidates are assigned a distinct symbol to represent the election and are entered into the blockchain. This automation and transparency makes sure the human intervention of the process is minimal and the information of the candidates is centralized.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

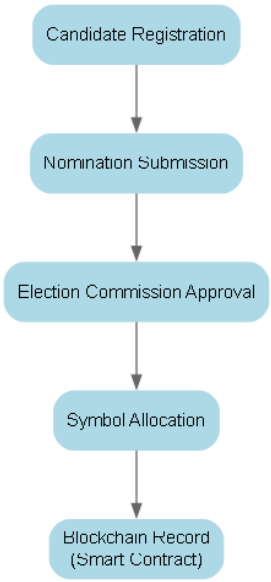

Fig 2 Candidate Module

C. Election Commission Module

This module acts as a management unit in the whole process of an election. This module has a role of verifying information of voters, candidates, and assigning symbols. After the voting process has been completed, this module will retrieve the information that has been saved in the blockchain to properly count the votes and announce the results. This module assists in auditing and validating the results, which is useful in determining anomalies in the process, and integrity of the results.

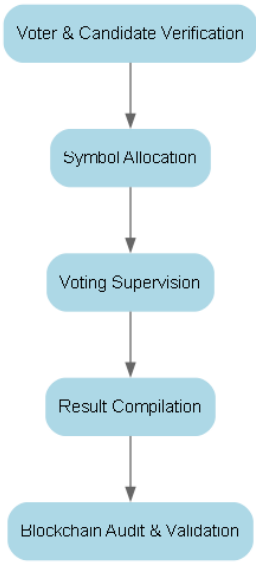

Fig 3 Election Commission Module

D. Hybrid Encryption Module

This module guarantees security of sensitive information in transmission and storage of information. This module applies AES as an efficient encryption tool of information and RSA as a key exchange tool. This module enjoys the advantage of symmetric and asymmetric key encryption in making information encryption efficient. This will guarantee the privacy and integrity of information despite the network threat and unauthorized access.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

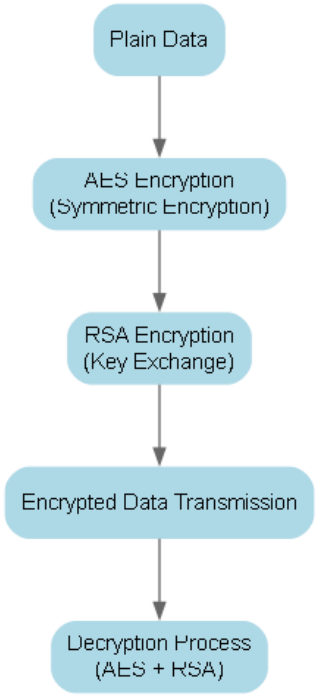

Fig 4 Hybrid Encryption Module

E. Blockchain Data Handling Module

The Blockchain Data Handling Module provides the decentralization, immutability and transparency of the election data. The Ethereum smart contracts are used to handle all key transactions in an election and the encrypted vote information are stored via the IPFS to enhance scalability and to minimize the storage expenses. The vote data content identifiers are saved in the blockchain to provide secure verification, audit, and resistance towards tampering data.

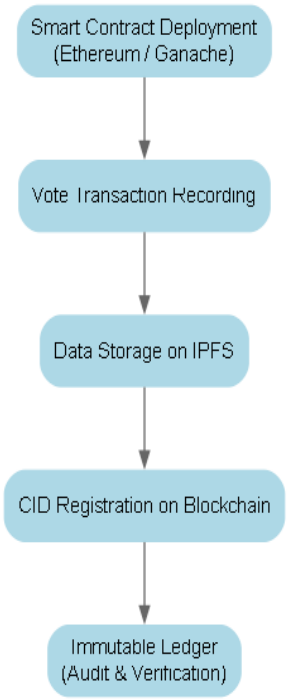

Fig 5 Blockchain Data Handling Module

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

VI. SYSTEM ARCHITECTURE

The system architecture of the proposed research, the BlockVote system, is decentralized, which guarantees the security, transparency, scalability, fault-tolerance, and reliability of the whole electronic voting process. The centralized control has been eliminated in the proposed system and the administration has been availed through the functional layers of the system with each layer addressing a particular aspect of the entire election process. The stakeholders in the Stakeholder Layer layer are the voters, the candidates as well as the election committee and, as such, they engage the system using the interfaces that are availed to them in the role of the stakeholders. The voters in the proposed system will be able to register, authenticate and cast their votes, the candidates will be able to make nominations and keep track of the voting process and the election committee will verify the votes, assign symbols, monitor the system and declare the results of the election. Authentication Layer provides secure and safe access to the system as a result of multi-factor authentication. It includes OTP based authentication and facial recognition with the use of the OpenCV. This will make sure that only qualified voters are able to enter the voting interface. This will avoid impersonation, duplicate votes, and unauthorized access. The Application Layer is in charge of the operations of the system. This involves voter registration, candidate registration and voting. The principle of election, i.e. one person, one vote is adhered to. The system also provides an assurance of votes that are cast over a given duration of time.

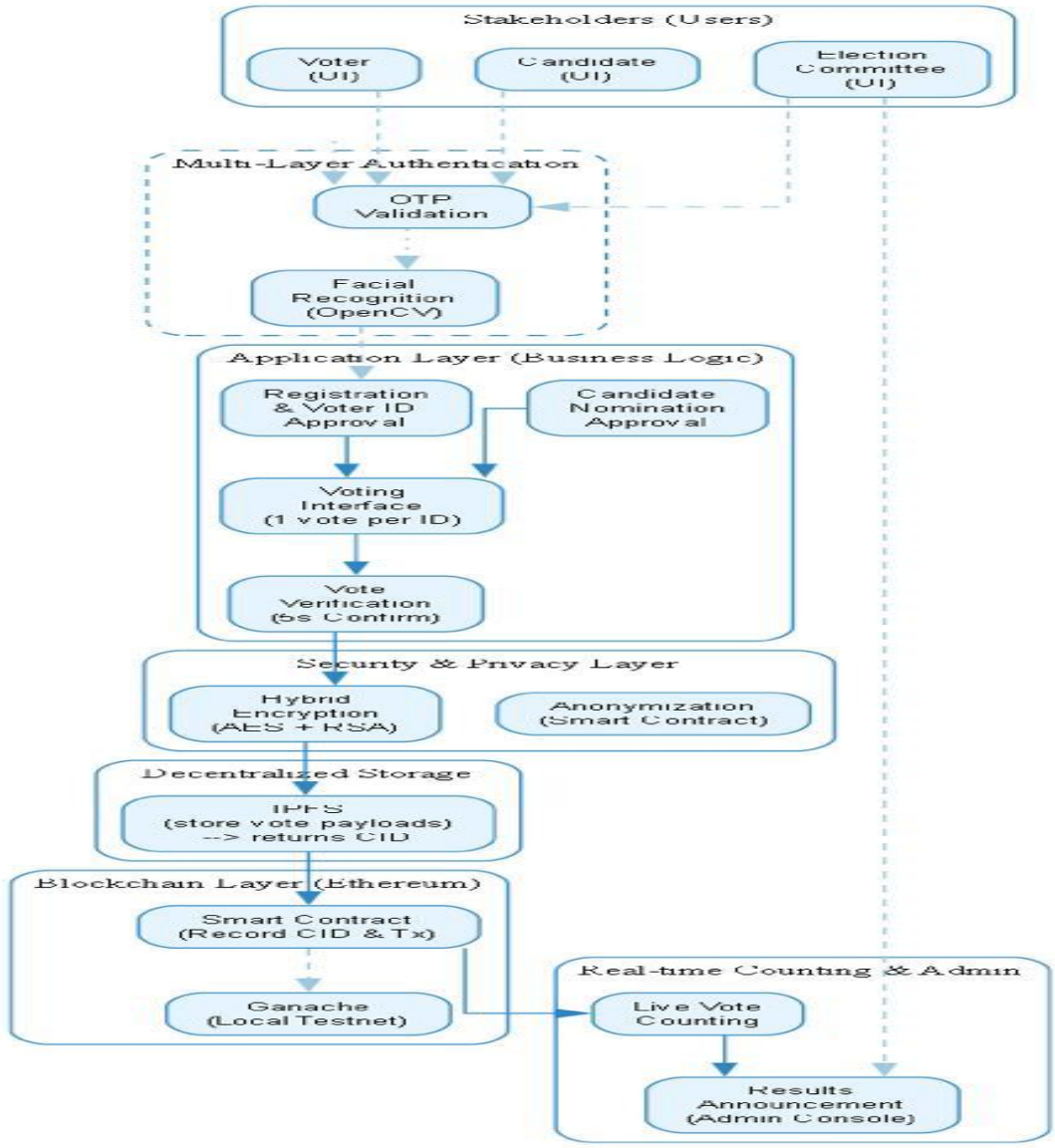

Fig 6 System Architecture

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

Security and Privacy Layer assures safety of the sensitive data by using a hybrid encryption method. This is through encryption of data using AES and key exchange using RSA. This guarantees confidential, integrity and authenticity of information.

The Decentralized Storage Layer involves InterPlanetary File System (IPFS) to encrypt and store vote data in immutable files with unique Content Identifiers (CIDs). This guarantees the information is available and that the people do not have single points of failure.

The IPFS CIDs are recorded in the Blockchain Layer which is developed with Ethereum smart contracts and Ganache. This makes the system to be scalable and at the same time the information to be tamper-proof, transparent and traceable.

Finally, the Real-Time Counting and Administration Layer performs counting and generation of results using the verified information that is utilized in the blockchain. This will guarantee the results are correct at all times and they cannot be manipulated once the voting process is done. This demonstrates that the suggested architecture is practical in offering a secure, scalable, and reliable solution to the dilemma of secure e-voting, which can be applied in the real world.

VII. SYSTEM METHODOLOGY

The process flow of the proposed system of BlockVote reveals how the processes related to the implementation of a safe, decentralized, and biometrically authenticated electronic election follow one another.

To begin with, the process of election configuration is initiated, in which the Election Committee sets the election process, nominates the candidates, designates the election symbols, and accepts the list of the eligible voters. The verification processes are all computerized in terms of accountability and to ensure that no one alters the information.
The process of the election configuration is followed by the availability of the system to execute the voting process.
The voter registration process comes before the actual voting process with the voter registering him/herself with the help of the web-based interface of the BlockVote system. The Election Committee has to verify the information that is provided by the voter as the identity and the voter will have access to the system.

The voter must be able to authenticate himself/herself on election day by using the OTP based authentication system along with facial recognition under the Open CV.

Once the authentication procedure is successfully completed, the voter is given access to the voting interface where he/she chooses his/her favorite candidate, and to avoid any form of accidental or repeated voting, there are voting restrictions, like the single vote rule and verification of the voting within a given time slot. Upon confirmation of the vote, it is anonymized to ensure the identity of the voter does not connect with the actual vote and therefore, the privacy of the voters is not compromised.

The secured vote is further encrypted under a hybrid encryption technique, where AES encrypts the vote data in an efficient manner, whereas RSA encrypts the AES-session key, which is then sent to the decentralized storage layer where it is stored in the IPFS as an immutable file. The vote information is encoded by the distinct content identifier, which is called CID, that is produced by IPFS.

Moreover, the CID is registered in the Ethereum blockchain in smart contracts, where the transaction is proven, and the CID is registered in an immutable register, where the real content of the vote remains concealed.

Lastly, the confirmed blockchain records are then utilized to perform the vote tallying in an automated fashion once the voting phase has ended, so that all reference to the votes will be unalterable and verifiable and the obtained results will be correct and impossible to interfere with once the election is over. The Election Committee can then announce the results in real-time and a complete audit trail can be used to check any dispute which might happen.

Overall, the given approach provides a safe and open election experience with the set of biometric authentication, cryptographic tools, distributed storage, and blockchain validation, which is why it can be used in the digital governance and elections.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

VIII. SECURITY ANALYSIS

Security of the proposed BlockVote system is assessed in regard to the high security risks that are commonly linked with electronic voting systems. Such risks are user impersonation, tampering of votes, duplication of votes and data leaks. The risks are addressed by incorporating the use of biometric authentication, hybrid cryptography, decentralized storage, and blockchain.

Multi-factor authentication is done using OTP authentication and facial authentication thus addressing impersonation of users. OTP authentication is applied to identify that credentials belonging to the user are in his/her possession whereas facial authentication is applied to identify that the user is affiliated to the registered voter. This multi-factor authentication system reduces the chances of user impersonation.

The fusion of blockchain and hybrid cryptography is used to deal with tampering of votes. The AES encryption is used in the encryption of the vote data whereas the key of encryption is the RSA encryption. After encryption, the vote data is saved to IPFS by storing it under a unique identifier called the Content Identifier (CID), and it will be saved on the Ethereum blockchain using smart contracts. As the blockchain transactions are immutable and have a unique reference point on any data stored in the blockchain network, any manipulation of the vote data will be easily recognized.

The prevention of the double voting implementation is executed both on the level of the application and the blockchain. This makes sure that the voting status flag of the valid voter is established hence preventing multiple votes to be cast. Besides, the smart contracts also ensure that the process of validating the transactions is done correctly thus disqualifying any duplicated votes. This makes sure that the one voter one vote rule is adhered to.

End-to-end encryption and identity vs. vote separation are applied to overcome the threat of data leakage. Here, the information of the voter and the votes are encrypted and sent to the store. Also, identity of the voter is separated with the content of the votes so that anonymity is guaranteed to the voter. The votes are encrypted and unreadable by the unauthorized parties that have access to the stored votes hence the confidentiality of the votes.

The decentralized design also avoids one point of failure that is usually created by centralized design of e-voting systems. The system ensures high availability and denial-of-service resilience by having a decentralized architecture that utilizes blockchain technology. Also, the IPFS encrypted data storage ensures long-term auditability. Moreover, the smart contracts allow imposing the rules in a transparent way.

Finally, biometric authentication, AES-RSA hybrid encryption, IPFS-based decentralized storage, and Ethereum blockchain technology would ensure that the e-voting system is secure, tamper-free, and privacy-conserving, and would be deployable in a practical manner.

IX. RESULT

This proposal was put into practice successfully to offer a decentralized web-based e-voting system with biometric authentication, hybrid encryption, IPFS, and Ethereum smart contracts. Functional and operational testing were also conducted to understand whether the proposed system was correct and working.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

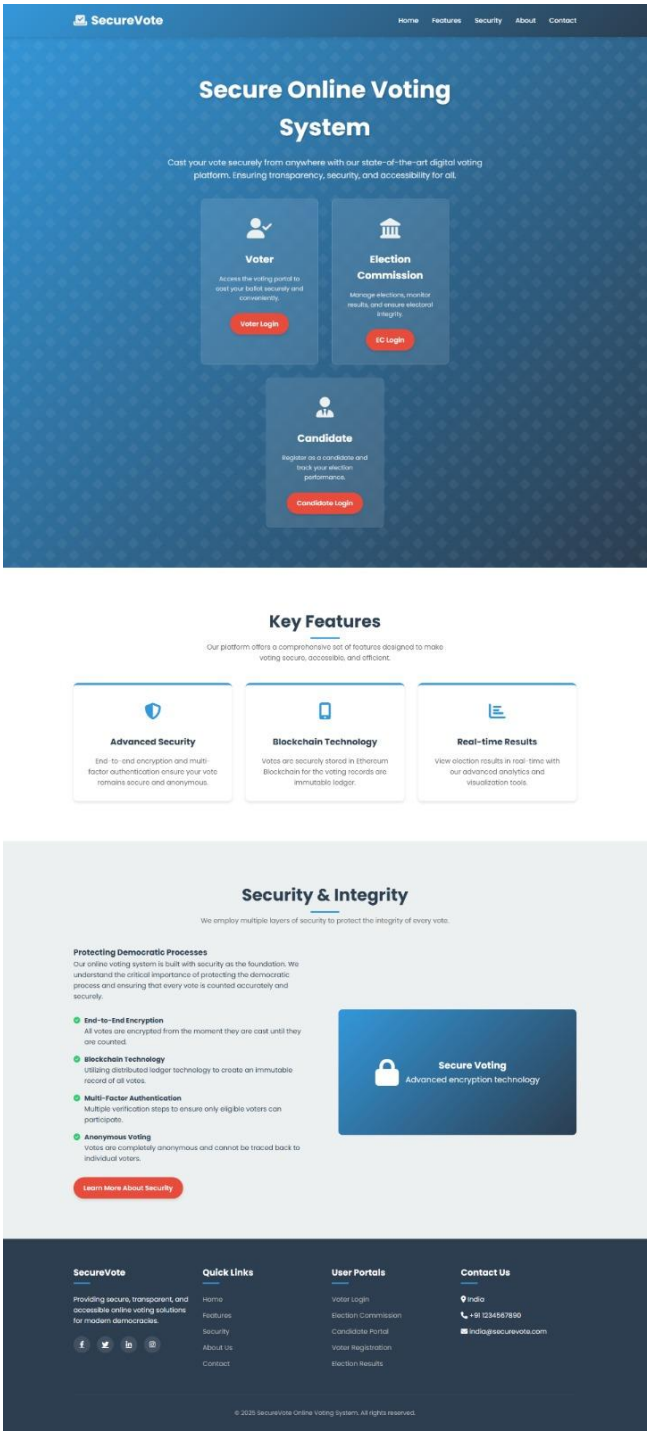

Fig 7 Main Interface

Voter registration and authentication modules have been taken through trial in different circumstances. The registered users could be authenticated using the OTP authentication mechanism. Also, the open CV-based facial recognition system could verify the identity of the voter and grant him access to the voting system. This proves the efficiency of the suggested multi-factor authentication system.

The hybrid encryption mechanism was used in encrypting some of the ballot information during the voting process. The vote payload could be efficiently encrypted by the AES encryption algorithm. Also, the session key of AES was

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

encrypted with the RSA encryption algorithm. The IPFS was used to store the encrypted vote files. Each vote had a unique Content Identifier (CID) created. Ganache test network and smart contracts were used to store these CIDs in the Ethereum blockchain. The transaction logs indicated successful execution and adding of vote information to mined blocks.

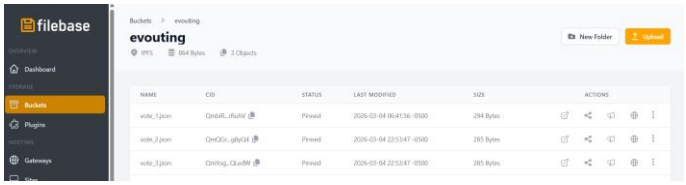

FIG 8 IPFS CID Generation for Encrypted Vote

Tampering of the stored vote data was done in order to test the integrity of the system. The blockchain, with its hash-related data, demonstrated CID incompatibility any time an IPFS data was altered thus preventing tampering of votes. The logic of the smart contract also worked well according to the prevention of voters voting more than once as they checked the status of the voters and then they could confirm the transaction which in turn effectively implemented the one voter, one vote principle.

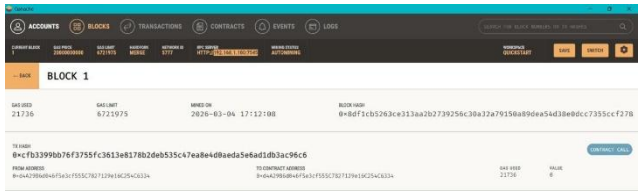

Fig 9 Blockchain Transaction Record in Ganache

The mechanism voting method was able to retrieve verified vote references of the blockchain data and calculate the results based on the operation of the smart contract. Results were generated without human interventions hence eliminating any form of vote manipulation after the elections. The real-time tracking option worked and enabled the Election Committee to see the voting process and outcome of the vote based on the blockchain information.

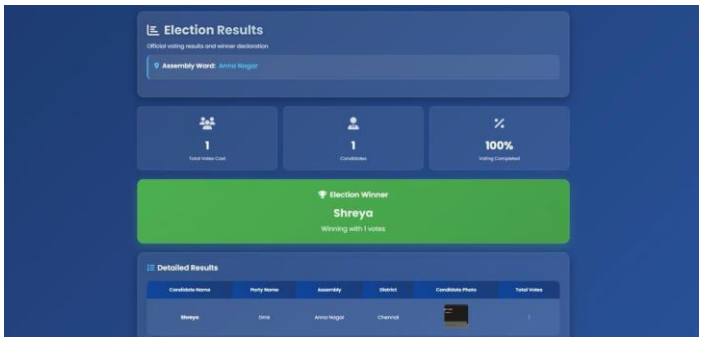

Fig 10 Real time vote count

In general, the implementation testing demonstrates the correctness and stability of the BlockVote framework in relation to each of the layers of functionality, including the authentication and encryption, as well as decentralized storage and recording on the blockchain and the results computation. The experiment demonstrates the potential of the use of biometric authentication together with the implementation of hybrid cryptography as well as the use of the blockchain as the means of holding the secure digital elections.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

X. FUTURE ENHANCEMENTS

Although the designed system of BlockVote will ensure the security and decentralized nature of the electronic voting process, some areas can be enhanced to ensure that the system itself is more efficient and effective. As an illustration, the system can be optimized in future to support large-scale implementations to support national or statewide elections of millions of voters. Advanced consensus algorithms and layer-2 scaling solutions could also be included to reduce transactional latency and network traffic to improve performance.

In addition, the authentication module will be expandable to multi-biological validation methods such as fingerprint and iris scanning to offer more accuracy on how identities are checked. Moreover, AI-based fraud detection methods can be included to detect abnormalities in real-time to discover suspicious voting behavior.

On the security aspect, the incorporation of post-quantum cryptographic should be able to offer a higher level of security against the threats of quantum-based attack in the future. In addition, compatibility of mobile platform can be designed to offer secure voting system through mobile applications.

Finally, the system can be integrated into the national digital identity framework and the government databases to ensure the usability of the system in real life by giving the voter verification more accuracy. This has the potential of making BlockVote a universal and extremely scalable digital election system.

XI. CONCLUSION

The paper has presented the notion of the decentralized and biometrically secured electronic voting system called the BlockVote. The necessity of a more secure and open electronic voting structure is a reaction to the problems that the security, transparency, and trust that relate to the traditional and centralized electronic voting systems.

The digital voting systems created and used by various nations in the world today are susceptible to the attacks of impersonation, vote manipulation, insider attacks and single-point of failure.

The proposed electronic voting framework combines the concept of multi-factor biometric authentication along with the application of hybrid cryptography and the blockchain to store the electronic and digital votes to resolve the challenges related to the security and transparency of the electronic voting systems.

The created prototype also demonstrates the practicality of the concept of blockchain technology and biometric verification integration into the actual application of digital elections. Functional testing was done to make sure that the vote could be safely cast and encrypted and stored in the blockchain ledger and results were calculated without any human intervention.

Altogether, BlockVote has offered a safe, decentralized, and transparent platform, which preconditions the development of the further electronic voting systems. The inclusion of the power of decentralized technologies and effective cryptographic protocols makes the digital electoral process more credible and dependable and thus is the step that will play a critical role in the democracies of the future.

REFERENCES

1. J. Mišić, V. B. Mišić, and X. Chang, “QPoS: Decentralized Stake-Based Leader and Voter Selection in a PBFT System With Mobile Voters,” IEEE Access, vol. 11, pp. xxxx–xxxx, 2025.
2. A. Alotaibi et al., “A Biometrics-Generated Private/Public Key Cryptography for a Blockchain-Based E-Voting System,” Future Generation Computer Systems, Elsevier, vol. xx, no. x, pp. xxx–xxx, 2024.
3. L. Ramesh et al., “Secure E-Voting System Utilizing Fingerprint Authentication, AES-GCM Encryption and Hybrid Blind Watermarking,” Journal of Advanced Engineering and Technology Studies (JAETS), vol. xx, no. x, pp. xxx–xxx, 2023.
4. P. Sharma et al., “Blockchain-Based Voting System Using Biometric Authentication,” International Journal of Innovative Research in Technology (IJIRT), vol. 9, no. x, pp. xxx–xxx, 2022.
5. K. Patel et al., “Blockchain-Powered E-Voting: A Novel Approach to Secure Voter Authentication and Election Automation,” in Proc. International Conference on Emerging Technologies, pp. xxx–xxx, 2024.
6. Y. Zhang et al., “An Efficient and Versatile E-Voting Scheme on Blockchain,” in Lecture Notes in Computer

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802045

Science, Springer, pp. xxx–xxx, 2024.
7. N. Kapsoulis et al., "Chirotonia: A Scalable and Secure E-Voting Framework Based on Blockchains and Linkable Ring Signatures," in Proc. IEEE International Conference on Blockchain, pp. xxx–xxx, 2021.
8. M. Hassan et al., "Blockchain-Based Secure Online Voting Platform Ensuring End-to-End Verifiability," IEEE Access, vol. xx, pp. xxx–xxx, 2024.
9. [9] J. Kim et al., "A Quantum-Secure and Blockchain-Integrated E-Voting Framework With Identity Validation," IEEE Transactions on Quantum Engineering, vol. xx, no. x, pp. xxx–xxx, 2025.
10. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
11. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
12. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
13. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
14. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
15. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
16. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
17. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
18. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
19. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
20. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
21. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
22. R. Singh et al., "EtherVote: A Blockchain-Based Electronic Voting System," Procedia Computer Science, vol. xx, pp. xxx–xxx, 2023.
23. H. Li et al., "E-Voting System Using Cloud-Based Hybrid Blockchain Technology," Journal of Cloud Computing, vol. xx, no. x, pp. xxx–xxx, 2024.
24. S. Verma et al., "DVTChain: A Blockchain-Based Decentralized Mechanism to Ensure the Security of Digital Voting Systems," International Journal of Information Security, vol. xx, no. x, pp. xxx–xxx, 2022.
25. A. Mehta et al., "E-Voting System Using Blockchain Technology and Homomorphic Encryption," International Journal of Cryptography and Security, vol. xx, pp. xxx–xxx, 2021.
26. K. Rao et al., "A Blockchain and Face Recognition Based E-Voting System," International Journal of Advanced Computer Science and Applications, vol. xx, no. x, pp. xxx–xxx, 2022.
27. F. Ahmed et al., "Hybrid-Blockchain-Based Electronic Voting Machine System Embedded with DeepFace and Post-Quantum Techniques," Sensors, MDPI, vol. xx, no. x, pp. xxx–xxx, 2024.
28. P. Kaur et al., "Blockchain-Based Voting System with Encrypted Ballots and Biometric Authentication," International Journal of Network Security, vol. xx, no. x, pp. xxx–xxx, 2023.