iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.78920

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Secure Blockchain E-Voting System with Biometric Authentication

Ms.Abirami K[1], Ms.Boomika K[2], Ms.Harshini M[3], Ms.Vaishnavi P[4], Mrs.Saranya S[5]
Department of Computer Science and Engineering N.S.N. College of Engineering and Technology Karur, Tamil Nadu, India

Abstract: ***E-voting systems have emerged as a promising alternative to traditional paper-based voting; however, concerns related to security, voter authentication, transparency, and trust continue to hinder their widespread adoption. This paper proposes a Secure Blockchain-Based E-Voting System with Biometric Authentication that addresses these challenges by integrating biometric verification with blockchain technology. The system ensures accurate voter identification through biometric authentication methods such as fingerprint or facial recognition, eliminating voter impersonation and multiple voting. Biometric data is securely processed with encryption and hashing, ensuring privacy and preventing unauthorized access. Once authenticated, voters cast votes electronically through a secure interface. Blockchain technology stores votes as immutable transactions within a decentralized ledger, making the system resistant to tampering and fraud. Smart contracts enforce election rules and automate validation and counting. This decentralized approach removes reliance on a single authority, enhances transparency, and enables real-time verification of results without compromising voter anonymity. The combination of biometric authentication and blockchain ensures a high level of security, integrity, and transparency throughout the election process, reducing the risk of electoral fraud and increasing voter confidence and participation.***

Keywords: E-voting, Blockchain, Biometric Authentication, Security, Transparency, Decentralized Ledger, SmartContracts

I. INTRODUCTION

Blockchain is a decentralized and distributed ledger technology that enables secure recording of transactions across multiple systems without a central authority. It operates on a peer-to-peer network, ensuring transparency and immutability of data. Blockchain's features, such as cryptographic hashing and consensus mechanisms, make it highly resistant to tampering. These properties are ideal for secure applications including e-voting.

Electronic voting systems facilitate the casting, recording, and counting of votes using digital technologies, aiming to improve efficiency and accuracy. However, traditional e-voting systems face challenges such as centralized vulnerabilities, data manipulation, and unreliable voter authentication. Maintaining voter privacy and data integrity, while ensuring transparency, security, and trust in the electoral process.

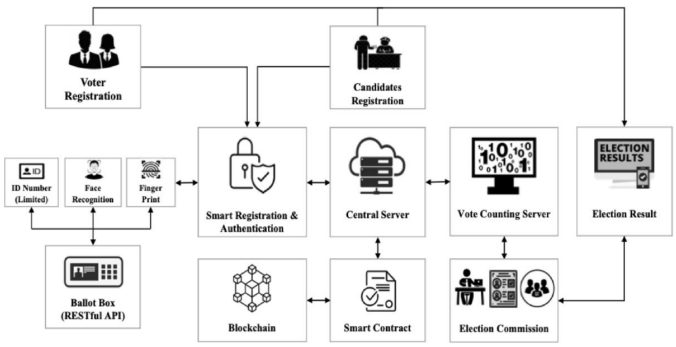


Fig 1 : Block Diagram

II. LITERATURE SURVEY

Over the past several years, researchers have made significant progress in developing blockchain-based electronic voting systems, often combining these technologies with biometric authentication to tackle security and transparency challenges.

For example, Kumar et al. introduced a voting platform that uses fingerprint verification to confirm each voter's identity and stores votes securely on a blockchain. Their resultsdemonstrated that this approach could greatly enhance transparency and minimize fraudulent activity during elections.

Similarly, Patel and colleagues designed a decentralized e-voting system, also built on blockchain technology, which incorporates biometric checks to ensure that each voter is uniquely identified. By encrypting and recording each vote as a blockchain transaction, their system was able to maintain vote integrity and effectively prevent tampering.

Chen et al. took a slightly different approach by integrating facial recognition into a blockchain voting system. The use of smart contracts for automatic vote validation and counting not only improved the security of the election process but also increased voter trust in the system.

Another noteworthy contribution comes from Singh et al., who developed a secure online voting solution that leverages both fingerprint authentication and one-time password (OTP) verification for multi-factor security. This design ensured that only authorized individuals could vote and that the confidentiality of the voting process was maintained.

Alshammari et al. focused on preserving voter privacy by combining blockchain with advanced encryption and zero-knowledge proof techniques. Their system allowed votes to be recorded immutably on the blockchain while keeping each voter's identity anonymous.

Collectively, these studies highlight the considerable benefits of integrating blockchain technology with biometric authentication in electronic voting. They show that such systems can strengthen both security and transparency. However, many existing solutions face challenges in terms of scalability and ease of implementation. The system proposed in this work aims to address these gaps by offering a practical, secure, and straightforward architecture suitable for real-world deployment.

III. EXISTING SYSTEM

Traditional voting systems are largely dependent on manual processes, including physical voter verification using ID cards and casting votes via paper ballots. While this method has been the default for decades, it is often slow, resource-intensive, and susceptible to human error. Manual vote counting can introduce mistakes, lead to disputes, and cause significant delays in announcing results. Additionally, physical ballots are vulnerable to loss, damage, or even tampering during handling and transportation.

With the aim of overcoming these limitations, electronic voting (e-voting) systems have been introduced. However, most existing e-voting platforms still rely on centralized servers and conventional authentication methods such as passwords or voter ID numbers. Centralized architectures create a single point of failure, making these systems attractive targets for hackers and increasing the risk of data manipulation or large-scale breaches. Unauthorized access to voting databases can result in the exposure or alteration of sensitive information, undermining the credibility of the election.

Authentication in many current e-voting systems is based on passwords or PINs, which are often weak, reused, or shared among users. These credentials can be easily stolen or guessed, leading to a high risk of voter impersonation. As a result, malicious actors may be able to cast votes multiple times or in place of legitimate voters, significantly compromising the integrity of the election process.

Another persistent issue is duplicate voting, where the same individual is able to cast more than one vote, either intentionallyor dueto system loopholes. Existing systems may lack robust mechanisms to detect and prevent such occurrences, further eroding trust in the results.

Transparency in vote counting is also a major concern. In many electronic and traditional systems, the counting process is opaque, and independent verification is difficult. This lack of transparency can lead to doubts, disputes, and decreased public confidence in the fairness of the outcome.

From a usability perspective, some existing systems are not easily accessible to all eligible voters. Requirements to appear in person at specific polling locations, use particular hardware, or navigate complex interfaces can exclude voters with disabilities, those in remote areas, or individuals with limited technical skills.

In summary, the main disadvantages of existing voting systems include:

- Vulnerability of centralized databases to hacking and manipulation
- High risk of vote tampering and unauthorized access
- Possibility of duplicate voting and voter impersonation
- Lack of transparency and limited verifiability in vote counting
- Slow, manual vote tallying and result declaration
- Security threats due to weak authentication methods
- No provision for real-time verification or auditability
- Limited accessibility for certain groups of voters

These challenges highlight the urgent need for more secure, decentralized, and user-friendly electronic voting systems that can guarantee the integrity, transparency, and reliability of elections.

IV. PROPOSED SYSTEM

The proposed solution presents a secure electronic voting system that leverages blockchain technology in combination with biometric authentication to address the limitations of traditional and existing digital voting platforms. This system employs both fingerprint and facial recognition techniques to verify the identity of each voter, ensuring that only authorized individuals are granted access to the voting process.

Once a voter's identity is authenticated using biometric data, they can proceed to cast their vote via a secure and user-friendly interface. Each vote is immediately encrypted and recorded as a transaction on the blockchain. By storing votes in blocks that are cryptographically linked to previous blocks, the system guarantees the immutability of the voting record—making it virtually impossible for any party to alter or delete votes once they have been cast.

Blockchain's decentralized architecture eliminates the need for a central authority, providing enhanced transparency and resilience against tampering or single points of failure. Smart contract logic is integrated into the system to automatically enforce election rules, such as ensuring that each voter can cast only one vote. Voters also receive real-time confirmation that their vote has been successfully recorded, further increasing trust in the process.

The administrative module supports a range of election management functions. Administrators can add and manage candidates, enroll or update voter information, monitor the progress of the election in real time, view live or final results, and generate comprehensive reports for auditing or analysis purposes.

The proposed system offers several key advantages over existing solutions, including:

- Robust security through the combination of blockchain and biometric authentication
- Tamper-proof vote storage and transparent, auditable vote counting
- Decentralized and distributed ledger, reducing risks associated with centralization
- Real-time result reporting and instant vote confirmation for voters
- Effective prevention of fraud, duplicate voting, and voter impersonation

By integrating advanced security mechanisms and user-friendly features, this system aims to provide a practical and trustworthy framework for conducting electronic elections at various scales.

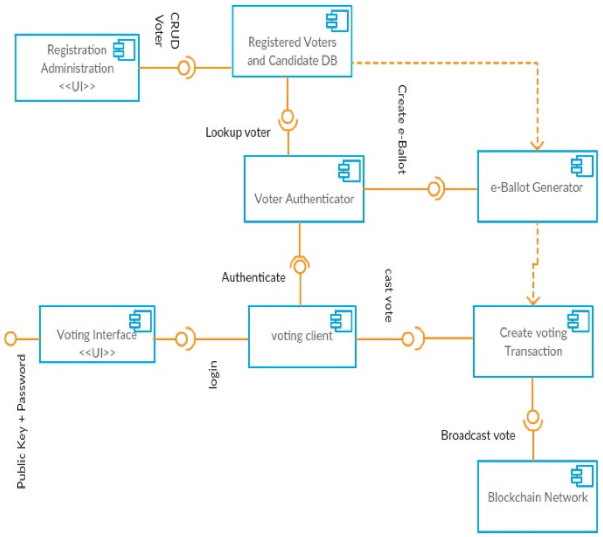


Fig 2 : Flow Diagram

V. METHODOLOGY

The proposed system adopts a step-by-step methodology designed to ensure secure, transparent, and reliable electronic voting using blockchain and biometric authentication. The workflow is as follows:

1) *VoterRegistration*
   Voters begin by registering on the platform, providing their personal details along with biometric data such as fingerprints or facial images. This critical step ensures that each voter's identity is unique and securely stored in the system.
2) *BiometricAuthentication*
   During the voting phase, voters are required to verify their identity using either fingerprint or face recognition. The system compares the provided biometric sample with the data collected during registration, ensuring only legitimate users can proceed.
3) *LoginVerification*
   After successful biometric authentication, the system also checks the user's login credentials for an added layer of security.
4) *VoteCasting*
   Authenticated users are then presented with a secure interface where they can select their preferred candidate from the list of options.
5) *VoteEncryption*
   Once a vote is cast, it is immediately encrypted using robust cryptographic algorithms. This guarantees the confidentiality and integrity of each vote.
6) *BlockchainRecording*
   The encrypted vote is then stored as a transaction on the blockchain. Each new vote becomes part of a block that is cryptographically linked to the previous block, creating an immutable chain of records.
7) *VoteValidation*
   The system enforces election rules—such as permitting only one vote per user—by employing smart contract logic. This prevents duplicate voting and ensures the integrity of the election.
8) *ResultCalculation*
   Votes are automatically tallied as they are recorded, eliminating manual counting and reducing the risk of errors or delays.
9) *ResultDisplay*
   After the voting period concludes, the final results are securely displayed to authorized users, providing transparency and real-time access to election outcomes.

This structured methodology not only addresses security and transparency concerns but also streamlines the entire voting process, making it efficient and trustworthy for both voters and administrators.

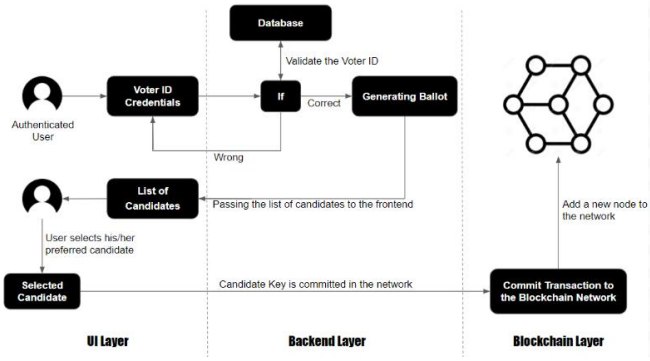


Fig 3 : Execution Diagram

VI. RESULTS AND DISCUSSION

The proposed electronic voting system was thoroughly tested to evaluate its effectiveness in real-world election scenarios. Biometric authentication, leveraging both fingerprint and facial recognition, was implemented to verify the identity of voters. During testing, the system consistently and accurately authenticated legitimate users, while attempts at duplicate voting or impersonation were promptly detected and rejected.

Once authenticated, each voter's ballot was encrypted and stored as a transaction on the blockchain. This approach ensured that no votes could be altered or deleted after submission, providing a tamper-proof and auditable record of every vote cast. The decentralized nature of the blockchain architecture further strengthened system transparency, allowing for independent verification and reducing the risk of centralized manipulation.

The system was also able to automatically tally votes as they were submitted, eliminating the need for manual counting and significantly speeding up the results process. Election administrators could monitor results in real time, and voters were provided with immediate confirmation once their vote was securely recorded.

Performance Analysis:

- The accuracy of voter authentication was significantly improved through the use of biometric verification.
- Vote tampering was effectively prevented, as all votes were immutably stored on the blockchain.
- The system successfully eliminated duplicate voting attempts.
- Results were generated much faster compared to traditional manual counting methods.
- Transparency was enhanced, as the decentralized ledger allowed for real-time monitoring and independent auditability.

Overall, the results demonstrate that integrating blockchain technology with biometric authentication can greatly enhance the security, reliability, and transparency of electronic voting systems. This approach not only prevents common threats such as vote tampering and impersonation but also streamlines the election process and builds greater trust among all stakeholders.

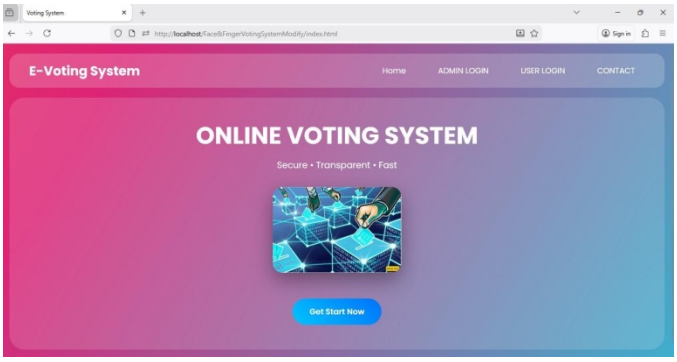


Fig 4 Home Page

Welcome to the Secure Blockchain E-Voting System—your modern, safe, and transparent platform for digital elections. Our system combines advanced biometric authentication and blockchain technology to ensure that only eligible voters can participate, while keeping every vote confidential and tamper-proof. Whether you're voting in college elections, organizational ballots, or larger government polls, you can trust that your voice will be counted accurately and securely.

With a user-friendly interface, quick registration, and real-time vote tracking, participating in elections has never been easier or more reliable. All votes are securely encrypted and stored on the blockchain, providing complete transparency and preventing fraud or duplicate voting. Start by logging in or registering as a new voter, and experience a secure, transparent, and trustworthy election process from start to finish.

Fig 5 : Admin Page

Welcome to the Admin Panel, your central hub for securely managing voters, candidates, elections, and results with the transparency of blockchain technology. The panel empowers administrators to register voters with biometric data, add or update candidate details, create and oversee elections, and monitor the entire voting process in real time. All votes are securely stored on the blockchain, ensuring data integrity and tamper-proof records, while results can be generated and published efficiently.

The Admin Panel is organized into intuitive modules, including Voter Management, Candidate Management, Election Management, Voting Monitor, Blockchain Storage, and Result Management. Security is at the forefront, featuring secure admin login, encrypted data storage, blockchain-protected votes, and biometric verification tracking. With everything accessible from one dashboard, you can run elections with confidence, ensuring secure control, transparent processes, and trusted outcomes.

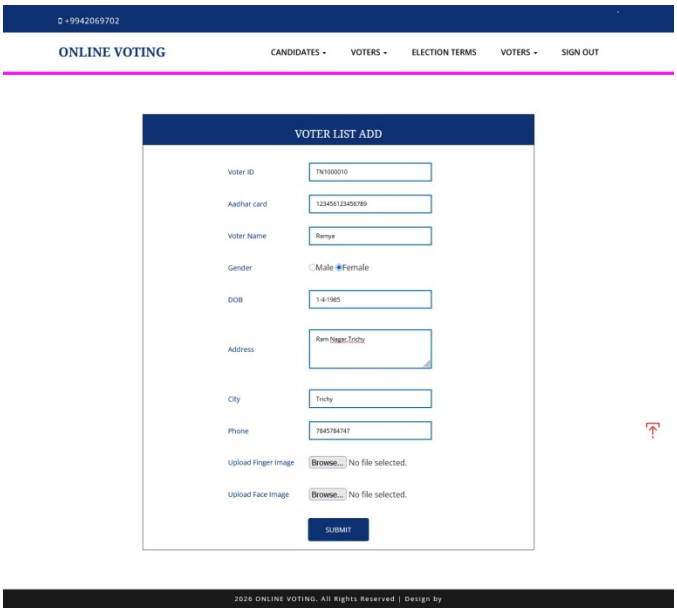


Fig 6 : VoterId Page

Welcome to the Voter ID Verification page. To begin, please enter your registered Voter ID and click the Verify button. You will then complete a secure biometric authentication step, ensuring that only eligible, registered voters can access the voting system and participate in the election.

Remember, each voter can vote only once. After successful verification, you'll be directed to the voting page. Any unauthorized or invalid Voter IDs will be denied access. This secure process guarantees fairness and transparency, upholding the principle of One Voter, One Vote for a truly secure election.

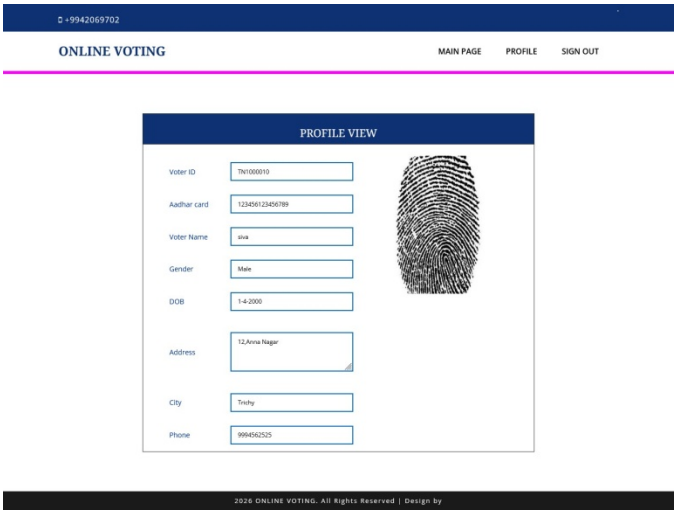


Fig 7 profile view

Welcome to your Voter Profile page, where you can review your registered details—including your Voter ID, name, contactinformation, and biometric verification status. All information here is securely stored and used solely for voter authentication and election purposes, ensuring your privacy and data protection at every step.

Your voting status is also displayed, letting you know whether you have already cast your vote. Once you submit your vote, the status will update and you will not be able to vote again. Please double-check your profile details before proceeding—this helps maintain a secure, verified, and trustworthy election experience.

VII. CONCLUSION

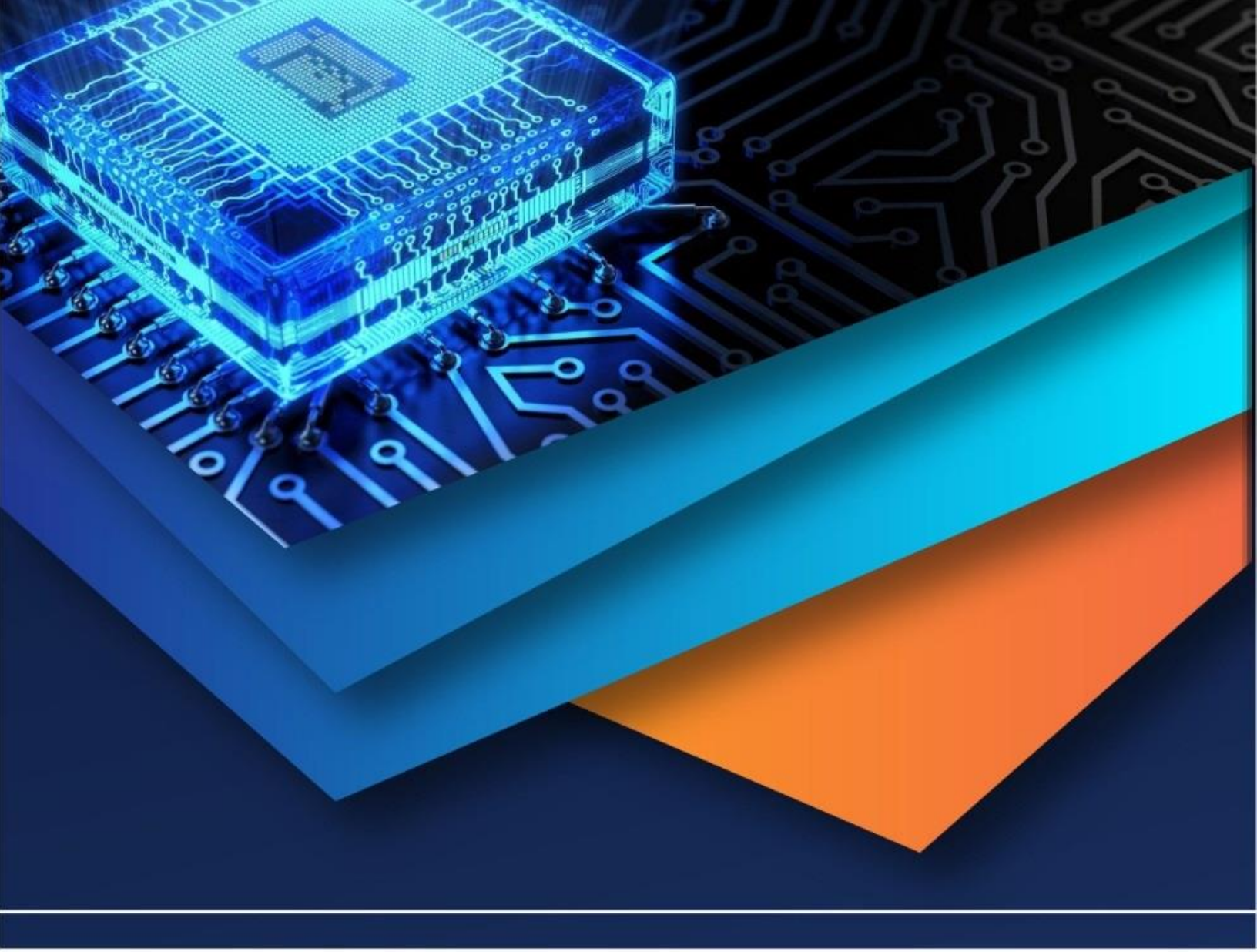
This paper introduced a Secure Blockchain E-Voting System that leverages biometric authentication to enhance the security and integrity of electronic elections. By combining fingerprint and facial recognition for accurate voter identification with blockchain's tamper-proof vote storage, the system effectively eliminates duplicate voting and prevents vote manipulation.

The decentralized architecture ensures transparency and removes dependency on central authorities, while real-time vote verification fosters greater trust in the election process. This solution is adaptable for use in college, organizational, and government elections.

Looking ahead, the system can be further improved by adding mobile voting support, deploying on cloud platforms, and integrating AI-based fraud detection to increase scalability and security.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[2] A. Kiayias, T. Zacharias, and B. Zhang, "End-to-End Verifiable Elections in the Standard Model," IEEE Symposium on Security and Privacy, pp. 468–482, 2015.
[3] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.
[4] K. M. Khan, J. Arshad, and M. M. Khan, "Secure Digital Voting System Based on Blockchain Technology," International Journal of Electronic Government Research, vol. 14, no. 1, pp. 53–62, 2018.
[5] F. Hao, P. Y. A. Ryan, and P. Zielinski, "Anonymous Voting by Two-Round Public Discussion," IET Information Security, vol. 4, no. 2, pp. 62–67, 2010.
[6] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT: Challenges and Opportunities," IEEE Communications Magazine, vol. 56, no. 10, pp. 112–117, 2018.
[7] R. Rivest and W. Smith, "Three Voting Protocols: ThreeBallot, VAV, and Twin," USENIX Workshop, 2007.
[8] D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, Stanford University, 2020.
[9] P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," International Conference on Financial Cryptography, 2017.
[10] S. Yi, Z. Qin, and Q. Li, "Security and Privacy Issues of Blockchain Technology," IEEE International Conference on Big Data, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY