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.2026.80056

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

Enhancing Electronic Voting Security Using Blockchain and Adaptive Biometric Authentication

Eluri Narmada, Chinnam Bhuvaneswari, Cheekurthi Devi, Rithin Gude, Gollapalli Venugopal, Arava Abhiram
Dhanekula Institute of Engineering and Technology(A) Vijayawada, India.

Abstract: ***Electronic voting systems have significantly improved the efficiency of electoral processes; however, challenges related to security, voter impersonation, and vote tampering still exist. This project proposes a secure and transparent electronic voting system that integrates biometric authentication with blockchain technology to address these issues.The system utilizes facial recognition as the primary authentication method and implements a fingerprint-based fallback mechanism using hash comparison to ensure reliable and privacy-preserving identity verification. Instead of storing raw fingerprint data, the system converts fingerprint inputsinto hashed representations, enhancing data security and preventing unauthorized access.Votes are recorded on an Ethereum-based blockchain using smart contracts, ensuring immutability,transparency, andpreventionof duplicatevoting. Eachvoteis stored asa secure transaction witha uniquehash, allowing verification while maintaining voter anonymity.Experimental results demonstrate that the system successfully provides accurate authentication, secure vote recording, real-time result updates, and effective prevention of duplicate voting. The proposed solution offers a scalable, secure, and trustworthy approach for modern digital voting systems.***

Keywords: Biometric Authentication, Blockchain, Electronic Voting, Face Recognition, Smart Contracts, Two-Factor Security.

I. INTRODUCTION

Due to their potential to increase efficiency, accessibility, and transparency, electronic voting systems are being investigated more and more as alternatives to traditional paper-based elections [1], [2]. One of the most important challenges in the design of contemporary electronic voting systems is ensuring both safe identity verification and tamper-resistant vote storage. Despite these benefits, trust in digital election platforms is still constrainedbyworriesaboutvotefraud,centralizeddata control, and voter authentication [3], [4].The use of blockchain technology to solve integrity and transparency problems indigitalelectionshasbeenthesubjectofrecent research[5].Forinstance,Kumaretal.suggestedEVOTE, adecentralizedblockchain-basedvotingplatformthatuses Solidity and React.js to record votes as unchangeable transactions on a blockchain network [6]. Their solution makes use of MetaMask to facilitate user engagement and guaranteesthatvotescannotbechangedaftertheyarecast. These decentralized systems lessen dependency on centralized authorities and enhance auditability. However, a lot of blockchain-based voting platforms, like EVOTE, rely mostly on wallet-based identification methods, which establish digital ownership but do not automatically validate voters' physical identities.

Research on electronic voting has progressively considered biometric verification techniques to improve voter authentication [7], [8], [9]. Compared to password-basedor wallet-based techniques, facial recognition and fingerprint authentication offer greater identity assurance [10].Thisstudysuggestsahybridelectronicvotingsystem that combines blockchain-based vote recording with adaptive biometric authentication [11]. Therefore, a workablevotingmechanismmuststrikeabalancebetween data confidentiality, usability, and identity assurance. However, adding biometrics creates new difficulties with regard to protecting templates, maintaining privacy, and safely storing sensitive information [12].

The main authentication method in the suggested system is face recognition; when facial matching confidence drops below a predetermined threshold, fingerprint verification is activated as a backup. This flexible method preserves stronger identity validation while enhancing usability. Before being stored, biometric templatesareencryptedusingAES-256-GCM,andhashed voter identities controlled by Ethereum smart contracts maintain vote uniqueness on-chain [11], [13]. Unlike systemsthatfocussolelyondecentralizedvotestorage,the proposed framework emphasizes both secure identity verification and immutable vote recording within a deployablearchitecture.Thesystemhasbeenimplemented andevaluatedinacontrolled blockchainenvironment,and performance metrics such as authentication latency, gas consumption, and transaction throughput are analysed to assessfeasibility.

©IJRASET: All Rights are Reserved

II. RELATED WORK

Research on tamper-resistant digital election infrastructures has been spurred by recent developmentsin distributed ledger technologies. In order to preventpost-election manipulation, a number of recent research have suggested decentralized voting platforms wherevotes are recorded as blockchain transactions. For example, EVOTE, a decentralized blockchain-based voting platform developed with Solidity and React.js, was presented by Kumar et al. [1]. Their method stores votes on a blockchain network to guarantee immutability and uses MetaMask for authentication. Although thesesystems successfully combat vote tampering and transparency, they mostly rely on wallet-based verification, which confirms digital ownership but doesnot intrinsically validate voters' real-world identities.

Biometric-based electronic voting systems have also beenproposed toimprovevoterauthentication[7],[8],[9], [12]. To lower the possibility of impersonation, certain digital voting prototypes have incorporated facial recognition and fingerprint verification procedures. Even though biometric authentication enhances identity assurance, a lot of these systems are still centralized and store private biometric information in backend databases without adequate security. Furthermore, few implementations explicitly address how blockchain-based immutability and biometric verification can be safely combined without revealing personal information.

Vote integrity and identity verification have been addressed via hybrid methods that combine blockchain technology with biometric authentication. Nevertheless, current frameworks frequently treat biometric identification as a required dual-factor procedure or concentrate mostly on theoretical models withoutthorough implementation and performance assessment. Limited studies provide empirical analysis of authentication latency, gas consumption, transaction throughput, and resistance to replay or double-voting attacks in a real implementation environment.

In contrast to prior work, the proposed system integrates adaptive biometric authentication with blockchain-based vote recording in a deployed architecture. Facial recognition is used as the primary authentication mechanism, and fingerprint verification is triggered only as a fallback when facial matching confidence is insufficient. Biometric templates are encrypted using authenticated encryption before storage, and vote uniqueness is enforced on-chain through hashed voter identifiers. Furthermore, this work provides detailed performance evaluation metrics, including authentication latency, smart contract gas consumption, transaction confirmationtime,andthroughputtesting,thereby offering a more comprehensive practical assessment compared to existing implementations.

III. METHODOLOGY

The methodology of the proposed voting framework is designed to ensure secure voter authentication, tamper-resistant vote recording, and controlled system scalability. The architecture integrates adaptive biometric verification with blockchain-based vote immutability while maintaining separation between identity management and on-chain data storage.

A. System Architecture

The overall system architecture consists of four primary components: the voter interface, backend processing unit, database and cache layer, and blockchain layer. As illustrated in Fig. 1, the voter interacts with the system throughaweb-basedinterface.Authenticationrequestsare processedbythebackendserver,whichmanagesbiometric verification, token generation, and vote validation.

Biometrictemplatesaresecurelystoredinanencrypted format within the database, while session and token management are handled through a caching mechanism. The blockchain layer includes a smart contract deployed on an Ethereum-compatible network, responsible for enforcingvoteuniquenessandmaintainingimmutablevote records.

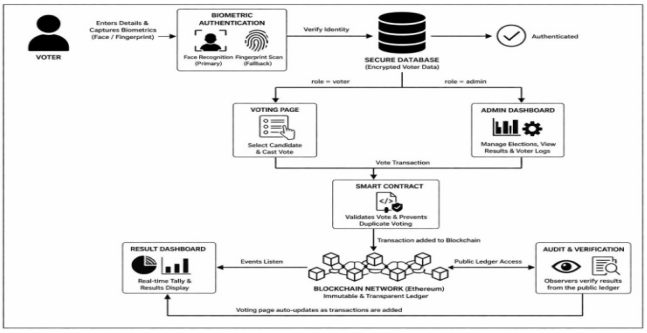


Fig. 1. System Architecture of the Blockchain-Based Voting Framework

B. Voter Registration

During the registration phase, each voter is assigned a unique identifier. Facial embeddings and fingerprint templates are captured and processed into feature vectors. Thesebiometrictemplates are encryptedusing AES-256-GCM with per-user derived keys before beingstored in thedatabase[4,13].Rawbiometricimagesarenotretained to minimize privacy risks.

C. AdaptiveBiometricAuthentication

On election day, facial recognition serves as the primaryauthenticationmechanism.Thelivefacialimageis compared with the stored encrypted template after secure decryption. If the confidence score meets the predefined threshold, authentication is successful.
If facial confidence falls below the acceptable threshold,fingerprintverificationistriggeredasafallback mechanism. This adaptive approach enhances usability while maintaining strong identity validation. Upon successfulauthentication,ashort-livedauthorizationtoken is generated to permit vote casting.

D. Blockchain-BasedVoteRecording

After authentication, the voter selects a candidate. The backend verifies election status and token validity before interacting withthesmart contract.Toenforceone-person-one-vote, a hashed voter identifier is generated using:

Hv=keccak256(voterID//electionID)

The smart contract checks whether the hashed identifier has already been voted. If unused, the candidate's vote count is incremented, and the identifier is marked as utilized. All transactions are recorded immutably on the blockchain.

E. SecurityandTransactionHandling

The system incorporates multiple security mechanisms to mitigate replay and duplicate voting attacks. JSON Web Tokens include expiration timestamps and unique identifiers.Tokensareinvalidatedimmediatelyafteruseto prevent reuse.
Blockchain transaction management includes nonce handling, dynamic gas estimation, and confirmation monitoring to ensure consistency between off-chain and on-chain states.

IV. IMPLEMENTATION

The proposed blockchain-based voting system was implemented as a full-stack web application integrating frontend, backend, database, caching, and blockchain components. The implementation focuses on practical deployability and secure integration between biometric authentication and smart contract-based vote recording.

A. Frontend Implementation

React.js was used in the development of the voter interface to create a user-friendly and responsive web application. Voter registration, biometric authentication, candidateselection,andresultviewingmodulesareallpart of the frontend. Using browser-based media APIs, the device camera is used to take facial images. RESTful API endpoints allow the interface to safely communicate with the backend. Additionally, an administration dashboard wasputinplace tooversee candidate registration,election configuration, and real-time vote tracking.

B. BackendandAPILayer

Ahigh-performancePythonframeworkwasusedinthe development of the backend server to manage token management, blockchain interface, biometric verification, andauthentication.APIendpointsweredesignedtohandle requests for registration, login, biometric verification, and voting.
JSON Web Tokens (JWT) with limited expiration timeswereusedtoimplementauthentiationtokens.Redis was utilized to control session data and stop token replay byinstantlyinvalidatingtokensfollowingvoteinput.AES-256-GCM is used to encrypt biometric templates prior to storage. A key derivation function is used to generate per-user encryption keys from a master key kept in environment variables. This guarantees that different encrypted outputs are produced from identical biometric templates.

C. DatabaseandCachingLayer

A PostgreSQL database was used to store voter metadata, encrypted biometric templates, and election configuration data. No raw biometric images are permanently stored. Only encrypted embeddings are maintained.Rediscachingwasintegratedtomanageshort-lived authentication tokens and to enforce single-use votingauthorization.Atomicoperationswereimplemented to prevent race conditions during concurrent vote submissions.

D. SmartContractandBlockchainDeployment

ThevotingsmartcontractwasdevelopedusingSolidity and deployed on the Ethereum Sepolia test network [1], [11]. The contract maintains candidate information and enforces vote uniquenessusing a mapping of hashed voter identifiers. To record a vote, the backend generates a hashed voter ID and signs a transaction using a dedicated backend wallet. Transactions are broadcast through a blockchain RPC provider. Gas estimation is performed dynamically before transaction submission to reduce failure probability. Transaction confirmation is monitored asynchronously, and voting status is updated only after successful receipt validation.

E. *DeploymentEnvironment*

The frontend application was deployed using a cloud-based hosting platform for continuous integration and globalaccessibility.Thebackendserverwasdeployedasa cloud web service integrated with a managed PostgreSQL database instance. Environment variables were used to securelystoreAPIkeys,databasecredentials,JWTsecrets, and private blockchain keys. HTTPS was enforced to ensure secure communication between client and server.

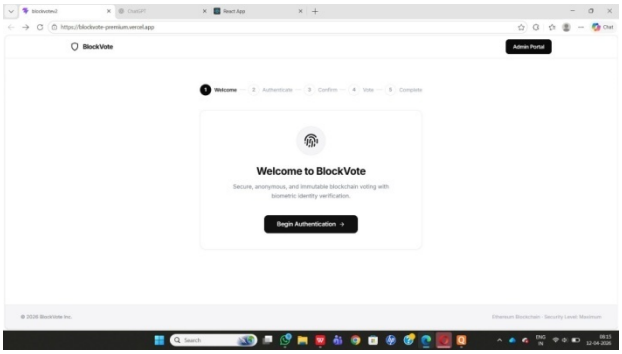


Fig.2.Illustratesthedeployedvotinginterface

V. RESULTS AND DISCUSSION

The proposed blockchain-based voting framework was evaluated in a controlled deployment environment to analyze authentication performance, transaction cost, throughput, and security robustness. Unlike conceptual models, the system was implemented and deployed usinga cloud-hosted frontend and backend integrated with the Ethereum Sepolia test network. The experimental observations provide practical insights into the feasibility of integrating adaptive biometric authentication with blockchain-based vote recording.

Theaveragefacialrecognitionauthenticationtimewas approximately 1.4 seconds under stable network conditions. Incaseswherefacialconfidencefellbelowthe predefined threshold, fingerprint verification wastriggered as a fallback mechanism, increasing the overall authentication time to approximately 2.2–2.4 seconds. When compared to wallet-based blockchain voting systems such as EVOTE [6], which rely on MetaMask signature validation and incur minimal authentication latency, the proposed system introduces additional processing time due to biometric verification. Although cryptographic wallets validate key possessions, they donot inherently guarantee physical voter identity verification. The marginal increase in authentication time in the proposed system therefore represents a practical trade-off for stronger identity assurance.

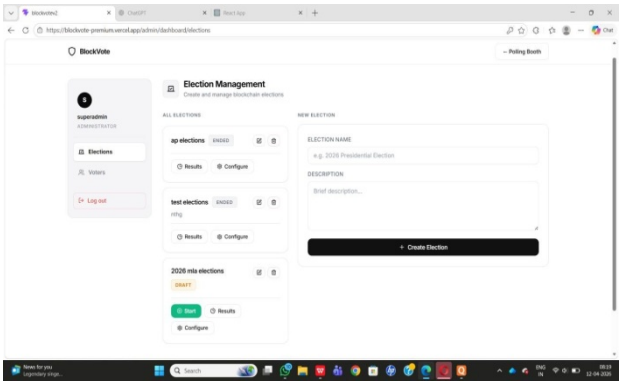


Fig.3.illustratestheelectionmanagementinterface

From a blockchain perspective, the smart contract required approximately 68,000–82,000 gas per vote transaction. This range is consistent with previously reported Ethereum-based voting implementations, where gas consumption typically varies between 60,000 and 100,000 gas depending on storage and mapping complexity [4], [11]. The optimized gas usage in the proposed design can be attributed to the use of hashed voter identifiers rather than storing extensive voter data on-chain. Although public mainnet deployment may incur higher financial costs during gas spikes, the measured values demonstrate feasibility for controlled or permissioned environments.

In comparison with previously proposed blockchain voting platforms, the results obtained in this study demonstrate improved identity verification and practical deployment feasibility. For example, decentralized voting systems such as EVOTE [1] record votes securely on the blockchain and ensure immutability; however, they primarily rely on wallet-based authentication, which verifiesonly digital ownership ofaprivatekeyrather than the physical identity of the voter. Similarly, several blockchain-based e-voting frameworks reported in recent literature focus mainly on vote storage transparency but depend on external authentication mechanisms that may still be vulnerable to impersonation.

The proposed framework addresses this limitation by integrating adaptive biometric authentication with blockchain-based vote enforcement. The experimental results show that although the system introduces slightly higher authentication time due to biometric verification, it significantly improves identity assurance while maintaining practical transaction throughput and gas consumption levels comparable to other Ethereum-based voting systems. Therefore, the proposed hybrid approach provides a more balanced solution by combining strong voter authentication with immutable vote recording, making it more suitable for secure and transparent digital election environments.

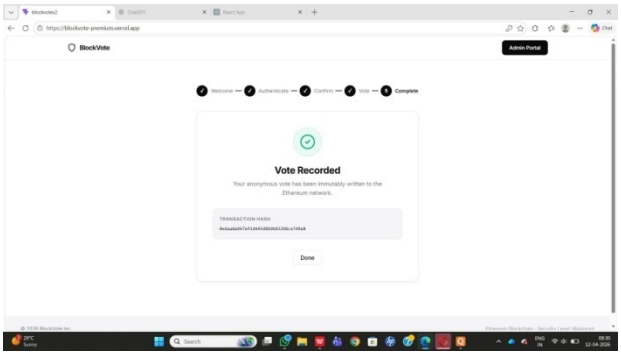


Fig.4.illustratesthesuccessfulvoting interface

Transaction confirmation time on the Sepolia network averaged between 3 and 5 seconds, depending on network congestion. This performance aligns with decentralized application benchmarks reported in recent blockchain research [3], [4]. Throughput testing under simulated concurrent voting conditions indicated sustainable processing of approximately 15–20 transactions per second. While centralized electronic voting platforms may achieve higher raw throughput due to absence of consensus mechanisms, they lack the immutability and distributed verification provided by blockchain networks. Thus, the observed throughput represents a balanced compromise between performance and tamper resistance.

TableIPerformancecomparison

parameter	Traditional VotingSystem	Proposed Blockchain–BiometricSystem
Authentication Mechanism	Manual ID verification	Facerecognition With fingerprint fallback
Result ProcessingTime	Hoursto Days (manual counting)	Nearreal-time (blockchain-based tally)
Tamper Resistance	Vulnerableto manual manipulation	Immutable blockchain

Security validation demonstrated effective prevention of duplicate voting, replay attacks, and unauthorized access. Duplicatevoteattemptswererejectedatthesmartcontract level through hashed voter ID verification, ensuring one-person-one-vote enforcement on-chain. [1], [3] Replay attacks were mitigated through nonce validation and immediate invalidation of authentication tokens. Compared to centralized biometric systems that relysolely on backend validation, the proposed system provides dual-layer enforcement through both backend verification and blockchain immutability.

Overall, the experimental results indicate that integrating adaptive biometric authentication with blockchain-based vote recording enhances election integrity with moderate computational overhead. The system maintains practical latency and transaction cost while significantly strengthening identity assurance and transparency compared to traditional or wallet-only blockchain voting systems.

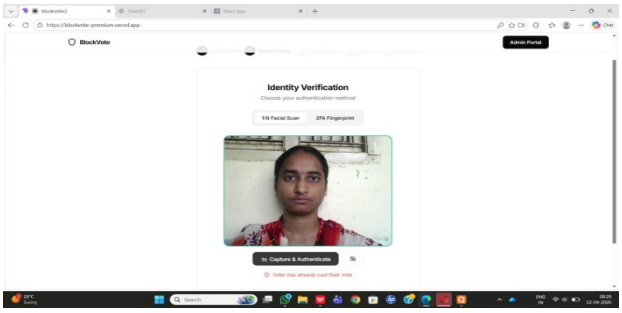


Fig.5.illustratestheeliminationofdoublevoting

The system prevents duplicate voting by verifyingthe voter's unique hashed identifier before recording a vote on the blockchain. If a voter attempts to submit avote more than once, the backend and smart contract validation mechanisms detect that the identifier has alreadybeenused and reject the request. Asshown inFig. 5, the system displays a notification indicating that the voterhasalreadyvoted,therebyenforcingtheone-person-one-vote rule and maintaining election integrity.

The experimental results demonstrate that theproposed blockchain–biometric voting framework provides a secure and practical approach for digital elections. The system achieved an average authentication latency of approximately 1.4 seconds for facialrecognition and up to 2.3 seconds when fingerprint fallback verification was required. Smart contract execution consumed approximately 68,000–82,000 gasper vote transaction, which is consistent with other Ethereum-based voting implementations. Transaction confirmationtime on the test network averaged between 3 and5 seconds,indicatingthat thesystem cansupportreal-time vote recording while maintaining blockchain immutability.

Overall, the implemented framework successfully prevented duplicate voting, replay attacks, and unauthorized access through combined biometric verification and smart contract validation. Compared with traditionalvotingsystemsandwallet-basedblockchain voting platforms, the proposed system demonstrates improved identity assurance, transparency, and tamper resistance while maintaining feasible computational and transaction overhead. These results confirm that integrating adaptive biometric authentication with blockchain technology can provide a reliable and secure solution for modern electronic voting environments.

VI. CONCLUSION AND FUTURE SCOPE

This research introduces a deployed hybrid electronic voting architecture that integrates adaptive biometric verification with blockchain-based immutability in a unified framework. In contrast to prior approaches that focus solely on either decentralized vote storage or standalone biometric authentication, the proposed system combines both components within a performance-evaluated implementation environment. Empirical results demonstrate that the framework ensures reliable identity validation, controlled gas expenditure, and stable transaction throughput while maintaining practical usability. These findings indicate that the integration of adaptive multi-stage biometric authentication with smart contract–driven vote uniqueness offers a scalable,tamper-resistant, and security-oriented enhancement over traditional and wallet-dependent digital voting solutions. Experimental evaluation demonstrated that the proposed framework achieves practical authentication latency (1.4–2.3 seconds), sustainable transaction throughput, and optimized gas consumption within a permissioned blockchain environment. Compared to traditional voting systems, the proposed model significantly improves transparency, tamper resistance, and result processing speed [1], [2]. In comparison with wallet-basedblockchain voting systems, it enhances real-world identity verification by incorporating biometric authentication rather than relying solely on digital signatures [5], [6].

While the proposed framework demonstrates practical feasibility and improved election integrity, several enhancements can further strengthen the system. One potential extension involves integrating hardware-based biometric devices, particularly real-time fingerprint scanners, to replace template-based fallback verification and improve authentication reliability in live election environments. Additionally, scalability can be enhanced through the adoption of Layer-2 blockchain solutions or rollup-based architectures to reduce transaction cost and confirmation latency during large-scale deployments.

Future research may also explore decentralizedidentity frameworks and privacy-preserving techniques such as zero-knowledge proofs to minimize centralized biometric custody while maintaining strong identity assurance. Further optimization of transaction batching mechanisms and distributed node configuration could improve throughput for high-volume voting scenarios. These advancements would enable the proposed hybrid blockchain–biometric architecture to evolve toward large-scale, privacy-preserving, and production-ready digital election systems.

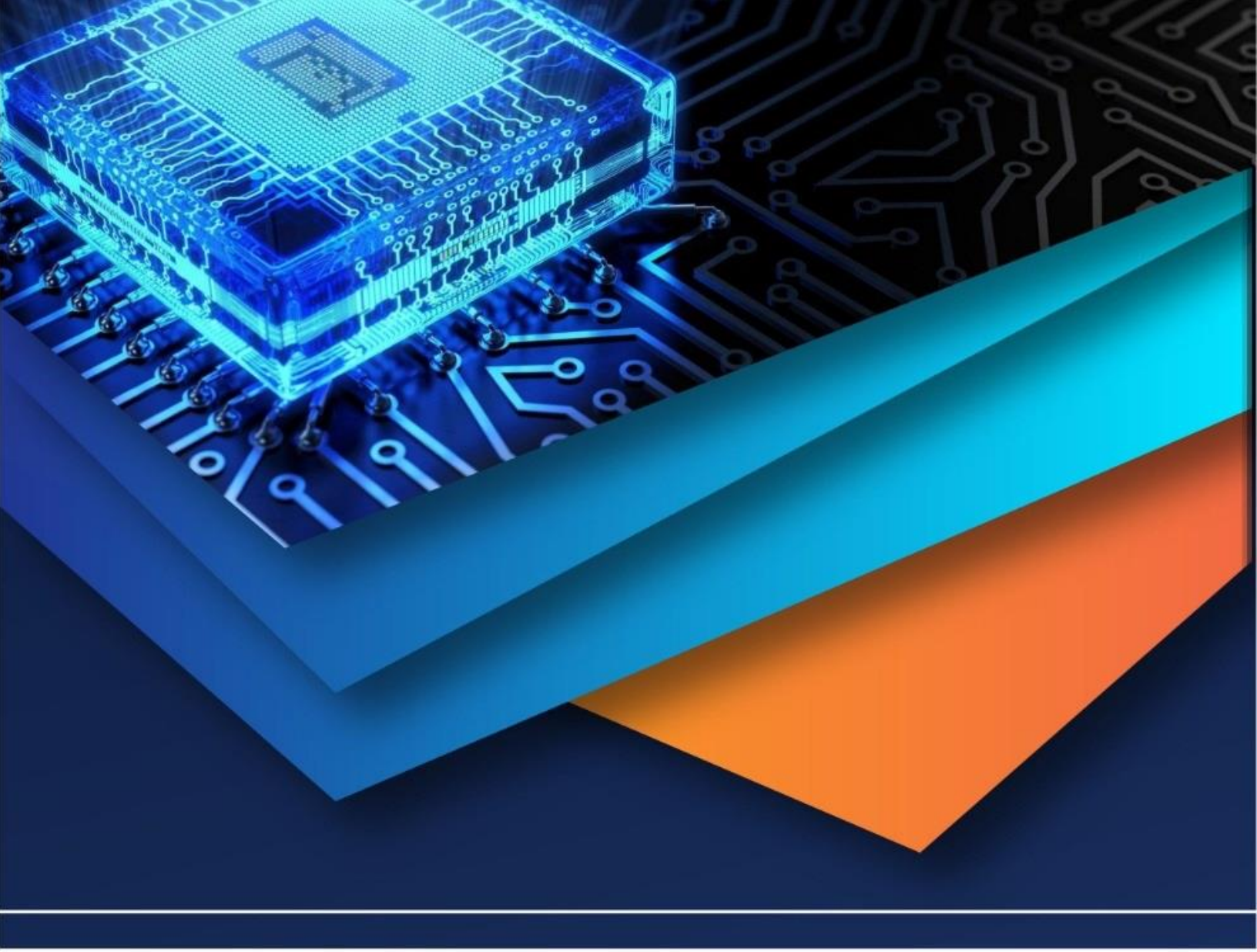
VII. ACKNOWLEDGEMENT

The authorswouldliketo extend theirsinceregratitudeto E. Narmada(AssistantProfessor)forprovidinginvaluable guidance, technical support, and continuous motivation throughout the course of this research. The authors arealso grateful to the Department of Computer Science and Engineering (AI & ML), Dhanekula Institute of Engineering & Technology, for providing the necessary academic environment, institutional support, and infrastructure facilities that enabled the successful development, deployment, and evaluation of the proposed blockchain-based secure voting system.

Theconstructivefeedback,technicaldiscussions,and encouragement received during various stages of the project significantly contributed to refining the system architecture, strengthening security mechanisms, and improving overall implementation quality.

REFERENCES

[1] S. V. Prasad et al., "Building Voting Systems for a Fairer Future: Exploring Blockchain based E-voting with EthereumforNationalElections,"IEEEPublication,2024. DOI:10.1109/icbds61829.2024.10837039
[2] A. Sharma et al., "Electronic voting system using blockchainandmachinelearning,"IEEEPublication,2024. DOI:10.1109/ic-etite58242.2024.10493453
[3] A. K. Goharshady and Z. Lin, "Blind Vote: Economical and Secret Blockchain-Based Voting," Proc. IEEE Blockchain 2024, 2024. DOI:10.1109/blockchain62396.2024.00016
[4] J. Huang, D. He, Y. Chen, M. K. Khan, and M. Luo, "A blockchain-based self-tallying voting protocol with maximum voter privacy," IEEE Transactions on Network Science and Engineering, 2022. DOI:https://doi.org/10.1109/TNSE.2022.3190909
[5] G. Vivekanandan et al., "VoteChain: Promising a Secure and Transparent Election using Blockchain and Biometrics," IEEE Publication, 2024. DOI:10.1109/icpects62210.2024.10780340
[6] Kumar,M.I.Choudhary,A.Singh,S.Kumar,and A. Abhishek, "Permissioned Smart Contract Based e-Voting System for University," Proc. IEEE NETCRYPT2025, 2025.DOI:10.1109/netcrypt65877.2025.11102528
[7] A.Kiran et al., "Secure Biometric Voting Systemusing Deep Learning and IOT," IEEE Publication, 2025. DOI: 10.1109/assic64892.2025.11158680
[8] S. Sandhya et al., "A Smart Voting System Using Biometrics and Embedded Systems," IEEE Publication, 2025. DOI:10.1109/icctdc64446.2025.11158827
[9] A. Manoj et al., "Next GenerationVotingApproach: A Secured Biometric Voting System," IEEE Publication,2024.DOI:10.1109/icicnis64247.2024.10823170
[10] P. Sidharth et al., "Securing Democracy: The Two- Phase Authentication Approach to Electronic Voting," IEEEPublication,2024.DOI:10.1109/icaaic60222.2024.10575389
[11] G. Mathur, P. S. Chauhan, P. Savita, S. Gupta, and P. Jain, "Securing the Ballot: Ganache's Role in Modernizing E-Voting," 2024 International Conferenceon Smart Energy Systems (ICSES), 2024.DOI:https://doi.org/10.1109/icses63445.2024.10763353
[12] 12.S. Sudha et al., "Biometric Smart Voting System Using Deep Learning with Internet of Things," IEEEPublication,2024. DOI:10.1109/mecon62796.2024.10776062
[13] Y.Yang,Z.Guan,Z.Wan,J.Weng,andH.Pang, "PriScore: Blockchain-based self-tallying election system supporting score voting," IEEE Transactions on Information Forensics and Security,2021. DOI:https://doi.org/10.1109/TIFS.2021.3108494



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)