iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.82385

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 V May 2026- Available at www.ijraset.com

VoteLedger: Blockchain-Integrated Secure E-Voting System with Transparent and Reliable Elections

Poonggazhal TTK, Dr. I. Shahanaz Begum, Amuthavalli G
Dept of Computer Science and Engineering, MIET Engineering college Tiruchirappalli , India

Abstract: ***The emergence of electronic voting is one of the vital components of contemporary democracies; however, guaranteeing security, transparency, anonymity, and integrity in this new medium is quite challenging in the current technological landscape. In light of this issue, this paper presents an approach for implementing biometric blockchain-based e-voting, which aims to eliminate the drawbacks of existing electoral processes. To be specific, the suggested model integrates facial recognition software for voter identification with blockchain for vote storage. In particular, to ensure reliable biometric identification, the suggested system utilizes the Grassmann algorithm, a mathematical technique used in high-dimensional feature spaces for comparing faces. When verifying the voter identity, a facial image is converted into a vector feature, after which the Grassmann algorithm computes the ideal subspace for matching the faces of registered voters. Such an approach enables highly precise authentication even under difficult conditions like variations in lighting, varied facial positions, or partial obstruction. Therefore, it can help avoid problems like duplication voting, impersonations, and other forms of electoral fraud. On confirming a voter's credentials, the vote cast is then encrypted and recorded as a unique voting transaction in the blockchain system. Each voting transaction gets a unique, cryptographic secure transaction ID, which makes it possible to track individual votes without breaching their privacy. With the use of blockchain technology, there is no need for centralized authorities and hence eliminates any threats associated with attacks from hackers, breaches by unauthorized parties, or any form of data manipulation. Moreover, smart contract systems are employed to automatically validate votes, detect anomalies, and reject any duplicate or invalid votes. Finally, once a valid vote is received, it is permanently recorded in the blockchain ledger, and the voter is notified about the transaction confirmation ID via secure channels like emails or SMS messages.***
Keywords: Authentication, Biometric, Blockchain, Encryption, Facial Recognition, Smart Contracts, Transparency.

I. INTRODUCTION

E-voting is now one of the significant elements of a contemporary democracy due to its improved speed, efficiency, accuracy, and convenience associated with the election process. Nevertheless, traditional e-voting is confronted with significant problems like data falsification, illegal access, opacity, and a lack of public trust in the results of elections. Centralized storage makes the system vulnerable to attacks, tampering, and possible failures of a single node of the database, hence, there is an evident necessity of implementing an alternative that would increase security and decentralization. It is possible to use the capabilities of blockchain technology to address these issues, since blockchain possesses immutability, transparency, traceability, and decentralization without requiring the involvement of any central entity. This works has the purpose at proposing a blockchain-based biometric voting system that allows the implementation of an innovative voting model that is transparent, secure, and verifiable. In the suggested framework, facial recognition is utilized as the biometric technique for authenticating voters, thereby enabling the system to recognize authorized voters and prevent unauthorized access, impersonation, and duplicate votes. All votes are represented as unique blockchain transactions, guaranteeing their permanence, traceability, and security. The distributed architecture provides an environment with minimized risk and greater accountability by eliminating centralized governance, which could be susceptible to corruption or fraud. Additionally, the application of blockchain technology together with biometric identification makes the voter authentication process highly reliable and secure. The developed platform integrates automatic validation and notification functionalities, which increase voter trust and satisfaction. Once the transaction is successfully confirmed following verification, a transaction identifier is provided to the user by sending it via email or text message. This information confirms the voter's participation in the process but does not disclose any voting preference or choice.

©IJRASET: All Rights are Reserved

A. Objectives

The main goal of this project is to create an effective, open, and secure electronic voting system that uses biometric verification together with blockchain technology. This solution will ensure that only eligible individuals will be able to vote by using precise facial recognition. It is important to mention that another goal will be to avoid any kind of double voting, impersonations, and unauthorized access. The other goal of this project will be creating a decentralized environment for voting that would record all voting transactions in the blockchain network in order to ensure that all voting actions will be documented and immutable. Data immutability and integrity will be guaranteed through the creation of a system that will document voting procedures without allowing any changes in the transactions once they are confirmed by the system. At the same time, the solution should ensure privacy of all voters and still allow transparency during voting procedure. Another goal will be creating public trust and traceability by providing unique transaction IDs for votes. Centralization avoidance will also be one of the goals of this project. The next goal is automation of validation processes via smart contracts for instant exclusion of invalid or suspicious votes. Moreover, the proposed project will address issues of ease in elections management as well as minimize human errors and reduce expenses associated with using conventional ways of voting. Accessibility and convenience for the users are other objectives that will be addressed within the project framework. The possibility of real-time monitoring and audit for authorities in charge of conducting elections will be another objective to consider. Moreover, it is crucial to make the platform scalable to meet the requirements in national or regional elections. Privacy will be another important objective to tackle within the framework of the project.

II. RELATED WORK

Kho, Heng & Chin., et al. [1], The literature provides a detailed review of cryptographic e-voting systems that give particular attention to security, privacy, and trustworthiness. The authors begin by providing some reasons for implementing the concept of e-voting in democratic countries. Some reasons include quick tabulation of votes, fewer human errors, better accessibility, and voter convenience. However, as the literature notes, the use of e-voting comes with some security and privacy issues that need proper attention. In this regard, the review systematically evaluates different cryptographic methods applied to protect the privacy of voters while maintaining other vital aspects of voting, including voter anonymity, ballot secrecy, vote integrity, accuracy, and fairness. The authors explore several cryptographic schemes such as homomorphic encryption, mix-nets, blind signatures, zero knowledge, and end-to-end verifiability to ensure that such cryptographic schemes help prevent some common attacks like vote tampering, impersonation, coercion, and replay attacks. The literature categorizes voting systems based on their architecture, such as centralized, decentralized, and blockchain voting systems. End-to-end verifiable (E2E-V) voting systems get special consideration since they enable both voters and observers to confirm that votes have been made as desired, recorded as cast, and counted as recorded without identifying voter identity.

HajianBerenjestanaki et al. [2] This research offers an overview of the technology and improvements within blockchain-based systems for online electronic voting. Firstly, the authors discuss the drawbacks and shortcomings of traditional voting systems. Specifically, they refer to the lack of transparency, security, and trust in these systems. In order to solve these problems, the authors highlight the possibilities associated with the use of blockchain technology. They discuss the problem of immutability of data in the blockchain and prevention of any changes made without permission. In addition, the researchers discuss the opportunities provided by the technology of distributed ledger in relation to ensuring transparency for all participants. Furthermore, different types of blockchains and the consensus mechanisms used in e-voting are discussed. Moreover, the advantages offered by smart contracts are also considered. Some difficulties, including scalability, security issues, and efficiency are discussed. Moreover, the architectures of various blockchain voting systems and their features are compared. Finally, the authors pay attention to some of the possible security threats related to this type of voting. The possibility of using blockchain technology allows increasing the degree of confidence in digital voting, eliminating the dependence on the central authorities. Burka et al. [3] The literature discusses an innovative AI-based methodology used for voting system analysis. The researchers consider how computer intelligence could be implemented in studying election-related data. The paper points out some limitations associated with conventional approaches to analyzing voting systems. Machine learning algorithms could be used in assessing the voting behavior and patterns. Various algorithms used for classification and prediction purposes are considered by the researchers. They include supervised learning algorithms. Moreover, the study discusses opportunities for optimizing election results using machine learning. Feature selection is one of the issues discussed in detail. Data preprocessing is another aspect of great importance for obtaining accurate predictions. Issues like model explainability and biased data could pose challenges for machine learning implementation. The authors note that machine learning techniques offer a number of opportunities for enhancing voting system research and policymaking in general. However, important issues should not be ignored, namely those related to ethics and data security.

Benabdallah et al. [4] In this systematic literature review, the use of blockchain technology to create secure systems for electronic voting is explored. The authors start by pointing out that there has been increased interest in blockchain technology in relation to secure electronic elections. The authors conduct an evaluation of available systems based on blockchain technology for e-voting. In the discussion, security issues such as transparency, integrity, and voter anonymity are considered. Blockchain technology is proposed as a way of providing a secure system without a central authority. Different implementations of blockchain used for electronic voting are considered. Public, private, and consortium blockchains are identified. Consensus algorithms are also discussed, along with cryptographic techniques that work well with blockchain technology. Problems associated with using blockchain for voting systems, especially in terms of scalability and efficiency, are mentioned. The authors discuss methods to preserve privacy in blockchain-based systems. Performance analysis of different systems is done.

Goldberg &Schär [5] The literature reviews governance systems within the decentralized autonomous organizations (DAOs). In this particular case, the authors evaluate voting systems applied in the metaverse environment. The study describes how blockchain-based governance works in virtual environments. The research sheds light on the use of the voting technique for making joint decisions in decentralized settings. Transparency and impartiality in DAO governance are the key aspects under analysis. Voting systems and participation models are evaluated using existing examples. The paper pays attention to the incentive mechanisms which impact the participation of voters in the process. Voting apathy, risks associated with governance centralization are considered as well. The research describes token-based voting systems and their strengths and weaknesses. The role of voter participation in decision making is discussed in the context of governance systems. Security risks connected with the governance token manipulation are reviewed. The study concludes that voting mechanisms in metaverse platforms are still evolving. The use of smart contracts for the automation of voting execution is mentioned as an example.

Rathee et al. [6] The above literature provides details on the design and development of an e-voting application leveraging the blockchain system within IoT-enabled smart city scenarios. The writers highlight the importance of creating a safe voting platform within the context of a connected urban infrastructure. The authors present a blockchain system that enhances the ease of voting. They explain why smart cities can gain from digital voting platforms. Security and confidentiality are considered vital factors within these environments. Transparency and protection are guaranteed through blockchain integration. Voting devices are used to authenticate voters and enable communication between them. Smart contracts are mentioned as essential tools that facilitate automated voting processing. Various challenges related to security threats and network scaling are discussed. The authors assess the efficiency and reliability of the system through its performance analysis. Cyber attacks and illegal access attempts are among the challenges examined.

Alvi et al. [7] The literature presents DVTChain, which is the name given to the blockchain-based decentralized approach proposed to strengthen security for digital voting purposes. In the context of research, the authors aim at tackling weaknesses inherent in traditional e-voting approaches. The research stresses decentralization in order to avoid having any points of failure within a system. Blockchain technology is used in order to guarantee immutable and transparent recording of votes. Cryptography is also incorporated into system design with the aim of preserving privacy of voters. Various means are mentioned by the authors to avoid tampering with votes as well as accessing any system. Smart contracts are applied in order to verify transactions involving voting activities. The paper also touches upon the aspect of protecting the system against attacks such as double voting. Scalability and efficiency performance evaluation of DVTChain are described. Faruk et al. [8]Bie-Vote is an effective framework developed by the authors for a secure voting system based on blockchain technology supplemented with biometric identification. As evident from the title, the main concern of the authors is to improve the mechanism of voter authentication. The use of biometrics for authentication purposes includes fingerprints and facial recognition. Transparency and integrity of vote registration are ensured by using blockchain technology. This voting scheme involves the use of biometrics in conjunction with blockchain technology. It is shown by the authors why combining the two technologies prevents any form of identity spoofing and double voting. The voting process is automated using smart contract technologies. Security aspects, particularly, those involving biometric data protection and storage, are discussed in detail by the authors. Vladucu et al. [9] The literature offers an extensive review of the e-voting systems based on blockchain. The study covers a number of different systems along with their architecture. The authors point out the progression from traditional to blockchain-based voting systems. The study focuses on the aspects of security, transparency, and scalability as main challenges. Different blockchain voting system categories are presented with relevant features. The study covers cryptographic mechanisms involved in blockchain voting systems. Advantages of these systems including decentralized nature and immutability are described in the literature. Limitations like scalability and computational expenses are also pointed out by the authors. Techniques of preserving voter privacy are critically reviewed. Multiple studies conducted on the topic of blockchain voting systems are compared by the authors. The literature emphasizes the necessity of end-to-end verifiability.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Varaprasada Rao & Panda [10] This literature describes an electronic voting system using blockchain technology, which operates on several platforms. This research emphasizes the necessity for security and transparency in voting in digital spaces. Blockchain technology is employed to guarantee the integrity of the data and protect it from any manipulation. Multi-platform compatibility is discussed in terms of usability and convenience. Voting processes are automated through smart contracts. Voter anonymity along with transparency is guaranteed by the authors. Cryptography is applied to secure the process of vote sending and storing. It allows removing the necessity of having centralized authorities within the process of voting. The issues of scalability and network performance are mentioned in the research paper. Performance testing is carried out on various computing platforms. The authors emphasize better reliability when compared to conventional methods.

III. PROBLEM STATEMENT

With the increase in the use of e-voting systems, the possibility of conducting fast and effective elections has been created; however, new problems related to security, transparency, privacy, and credibility have arisen. Many traditional e-voting systems use centralized database structures, where there is the risk of hacking and other attacks, unauthorized access, manipulations with information, or failure. All this makes conventional e-voting insecure, reduces people's confidence in the election, and undermines its integrity. In addition, in many existing systems, there is no reliable mechanism for voter authentication, which poses a threat to voting because there are possible dangers of voter impersonation, duplicate voting, and voting by non-residents. Manual verification is ineffective and requires much time and can be performed incorrectly. Moreover, modern systems cannot guarantee the transparency of voting, meaning that they do not allow verifying whether all votes were counted and recorded properly. Thus, preserving anonymity and, at the same time, being accountable in digital elections is very challenging. In view of the growth of cyber attacks, conventional voting systems become increasingly insufficient for conducting reliable elections. Therefore, the necessity to create an efficient e-voting system with the integration of biometric and blockchain technologies arises.

IV. PROPOSED METHODOLOGIES

The new system referred to as the Vote Ledger(Figure 1) is created with the purpose of developing an electronic voting mechanism that guarantees security, efficiency, and transparency through the use of biometrics and blockchain technology. Its primary aim is to facilitate voting only among authenticated individuals and at the same time eliminate any forms of fraud and privacy concerns along with fast results processing of the elections. Voter registration is the first process that is done in this system whereby each voter's facial image is acquired and stored in the database. In this process, the facial images are analyzed using the Grassmann algorithm and high-dimensional feature vectors are mapped into optimal subspaces. This ensures the verification of faces regardless of the light source, face pose, and partial occlusions. With proper authentication, voters can then cast their votes using the digital platform safely. Every vote cast by users of the voting application will be encrypted and recorded as transactions on the blockchain ledger. The blockchain ensures that every single vote made is immutable, transparent, and traceable without compromising the anonymity and integrity of voters. Voting applications make use of smart contracts to verify voter activities as well as identify any suspicious voter transactions in real-time. Any duplication or unusual activities that attempt to compromise the integrity of votes are rejected by the application. Once votes pass the verification process, they will then be recorded permanently on the blockchain network. Users will receive transaction IDs as proof of their votes via trusted communication platforms such as emails or text messages. The platform also provides real-time voting results since votes will be counted once polls close. In addition, decentralized architecture guarantees security by eliminating any reliance on centralized servers, thus making it difficult for any form of cyber attacks.

V. METHODOLOGY

A. Voting Interface Creation

The voting interface is the front-end platform where voters interact with the system to cast their votes securely. It is designed with a user-friendly layout to ensure accessibility and ease of use for all participants. The interface allows voters to log in, view available candidates, and cast their votes seamlessly. Security features such as session management and encrypted connections ensure that no unauthorized individual can access or manipulate the voting process.

B. Add Candidate Details

This module allows the election administrator to add and manage candidate information within the system. Each candidate’s name, party affiliation, symbol, and other relevant details are securely stored in the blockchain to maintain transparency and prevent unauthorized changes. The data entry process is verified and validated before being added to the blockchain ledger, ensuring authenticity and integrity of candidate information throughout the election period.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. User Credentials

The system assigns each registered voter a unique digital identity and login credentials. These credentials include a secure username, password, and encrypted biometric data such as facial features. This ensures that only eligible voters can access the voting interface. All credential information is encrypted using cryptographic algorithms, preventing data breaches or misuse. Before a voter can cast a vote, their identity is verified through biometric authentication, typically using facial recognition technology. Once verified, the voter is granted access to the polling section where they can select their preferred candidate. The system ensures that each user can vote only once, adhering to the "one-person-one-vote" principle. The polling process is recorded as a blockchain transaction to ensure traceability and prevent tampering.

D. User Verification and Polling

Before a voter can cast a vote, their identity is verified through biometric authentication, typically using facial recognition technology. Once verified, the voter is granted access to the polling section where they can select their preferred candidate. The system ensures that each user can vote only once, adhering to the "one-person-one-vote" principle. The polling process is recorded as a blockchain transaction to ensure traceability and prevent tampering.

E. Blockchain Implementation

Blockchain serves as the backbone of the system, ensuring decentralization, transparency, and immutability of all voting transactions. Each cast vote is stored as a unique transaction on the blockchain, protected through cryptographic hashing and verified by network nodes. Smart contracts are used to automate validation, counting, and result generation processes. This decentralized approach eliminates any single point of failure and prevents vote manipulation or data alteration.

F. Result Announcement

Once the voting period ends, the system automatically compiles and tallies the votes stored in the blockchain. The final results are generated using smart contracts that count only verified and validated votes. Since the data is immutable and transparent, the announced results can be publicly verified without compromising voter privacy. This ensures full trust, accuracy, and fairness in the election outcome.

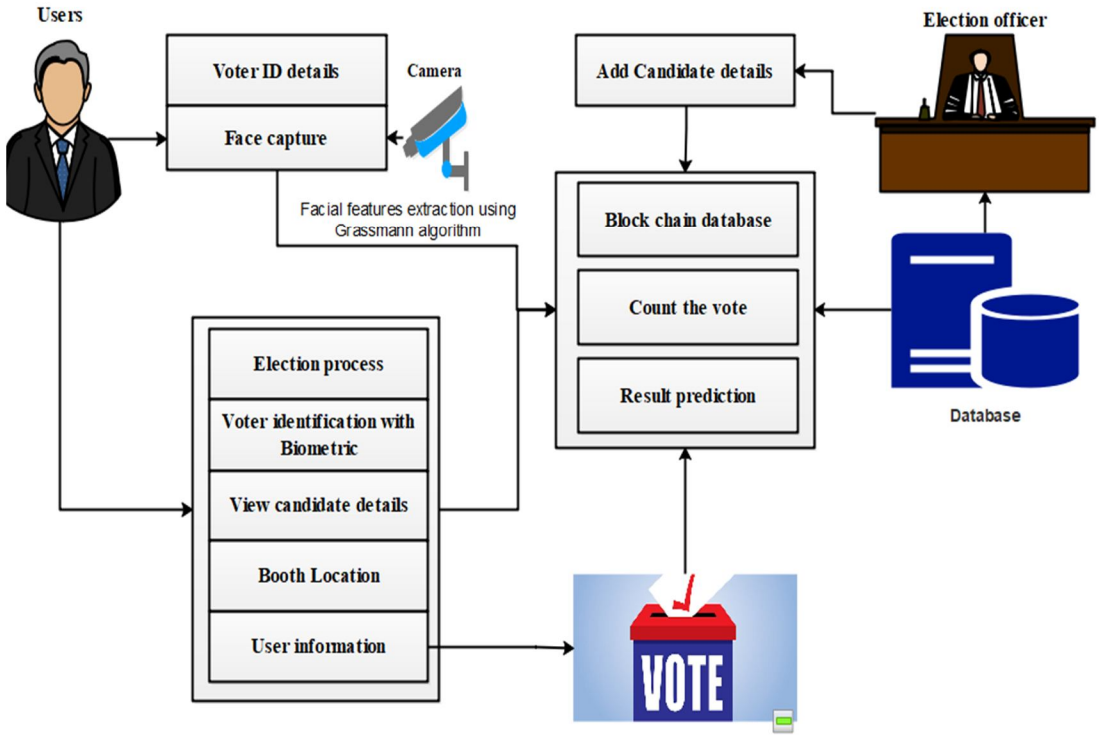


Figure 1: Diagram representation of the proposed methodology

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

VI. IMPLEMENTATION DETAILS

The Vote Ledger system implementation involves using an integrated software framework, which includes modules for biometric authentication, blockchain network, database management, and user interface. The proposed Vote Ledger system has been implemented in Python, along with the use of frameworks such as Flask or Django for web applications, and other libraries including OpenCV, NumPy, and Scikit-learn for handling facial images. In the registration process, the details and images of voters are collected using a secure interface and are saved in an encrypted database. Facial images collected from voters are subjected to preprocessing techniques such as image resizing, conversion into grayscale, normalization, and filtering noise. Feature extraction is then done by applying the Grassmann algorithm, which transforms facial images into high-dimensional feature vectors and projects them to optimal subspaces. In the voting stage, the voter logs in and undergoes biometric authentication using either live video feed from a webcam or an uploaded facial image. After a successful authentication procedure, the voter gets access to the voting portal and selects his or her preferred candidate. The selected vote is encrypted and transformed into a blockchain transaction. A blockchain platform like Ethereum, Hyperledger, or even a private distributed ledger will be used in the implementation of the blockchain layer. This layer facilitates the use of smart contracts to automate voter verification, avoid duplicate voting, conduct transaction validations, and keep the votes stored in a tamper-proof manner. Every time a vote is cast, there is the generation of a unique transaction identifier that is sent to the voter via secure means like e-mail or SMS API services. There is an admin interface for election tracking, voter management, candidate management, and viewing of results live during the election process. There are tests done for checking the accuracy of authentication, transaction speeds, security, and scalability due to multiple voting requests.

VII. EXPERIMENTAL RESULTS

Based on the findings of the experiments conducted on the proposed Vote Ledger model, there is high security, authentication accuracy, efficient transactions, and reliability of the e-voting system. This system was tested through a dataset of facial images of registered voters subjected to various environmental conditions such as lighting, pose, and partial occlusion to assess the effectiveness of the Grassmann algorithm used in biometric validation. High accuracy was obtained during authentication, allowing only the rightful voters to be authenticated, and preventing other users from voting. In the simulation test, all confirmed votes were encrypted and registered in form of transactions on blockchain with no data loss and tampering. Blockchain technology ensured data integrity and transparency in relation to the voting procedure from start till the end of the experiment. Smart contracts helped validate incoming votes while discarding suspicious, duplicate, and invalid transactions automatically. Time spent on verifying transactions remained low so as not to slow down users during the vote casting process. Scalability tests proved that the solution had good capacity even at high loads when a large number of people used it simultaneously. Instantaneous result tally was performed with success as well; it became possible to generate results as soon as the voting period finished. Transaction IDs were generated properly and then sent to voters via e-mail or SMS. The comparative assessment of the proposed platform in relation to traditional online voting systems revealed that it provided higher security against fraud, guaranteed greater data integrity and transparency. The distributed nature of the system decreased risks of server crashes and database manipulations. According to user satisfaction surveys, people enjoyed using the voting app because of its convenience and fairness.

Performance Metric	Existing System (%)	Proposed System (%)
Authentication Accuracy	88.40	97.65
Vote Security	84.75	98.20
Fraud Detection Rate	82.60	96.90
Data Integrity	86.30	99.10
Transaction Success Rate	87.25	97.85
Voter Privacy Protection	83.90	96.75
Real-Time Result Efficiency	85.15	95.60
Overall System Reliability	86.50	98.05

Table 1: Performance Comparison Table

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

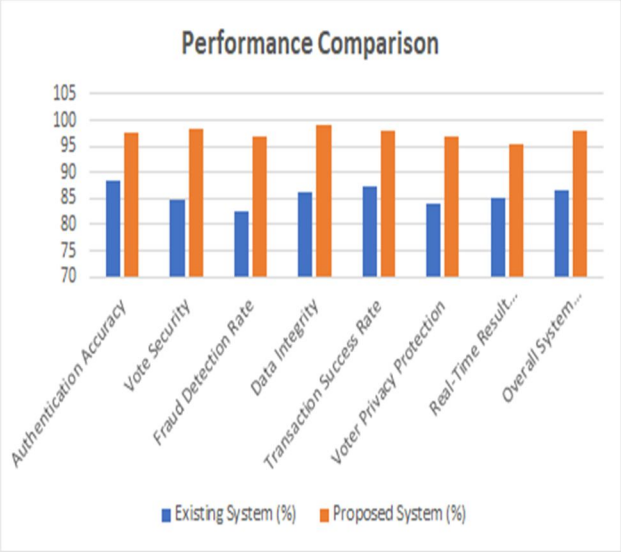


Figure 2: Performance metric chart representation

As evident from the performance comparison in terms of metrics(Table 1, Figure 2), the combination of biometric identification and blockchain technology brings several key benefits for Vote Ledger in comparison with the current system of e-voting. The current system is characterized by average performance, since its main elements involve centralization, conventional logins, and insufficiently developed protection against any forms of fraud or system manipulation. At the same time, the new Vote Ledger managed to significantly improve the performance of authentication by implementing facial recognition with the help of Grassmann algorithm, thus ensuring that only legitimate and registered voters can take part in the voting process. Another significant performance improvement in Vote Ledger is associated with the high level of data security, since all votes are protected with encryption and become immutable transactions in the blockchain. Finally, it should be noted that the performance in terms of fraud detection is also higher due to real-time smart contracts, which identify and reject all duplicate and questionable votes. In comparison with the current system, the proposed model enhanced voter privacy because it ensured separation between voter identification and their choice while maintaining the transparency of transactions via unique transaction IDs. Voting result efficiency was also better because the results were calculated real-time upon transaction validation on the blockchain, and final results could be declared without any delay. The reliability of transactions and the system itself were also higher in terms of success rates thanks to the decentralized nature of the technology, which does not have a single point of failure and therefore depends less on central servers. Besides, the scalability of the system was improved in case of many simultaneous voters. Altogether, the comparison showed that the proposed Vote Ledger system was superior to the conventional e-voting system in all aspects such as security, transparency, accuracy, privacy, efficiency, and reliability.

VIII. RESULT



Figure 3: Home Page

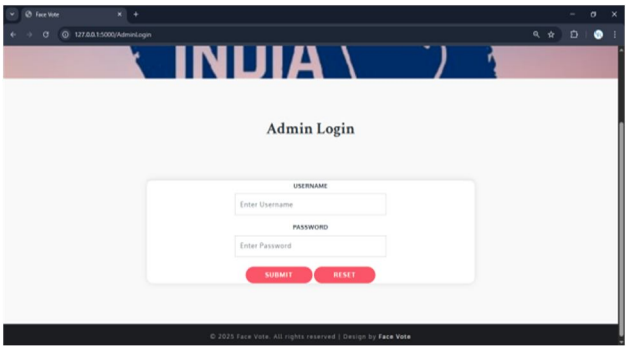


Figure 4: Admin Login Page

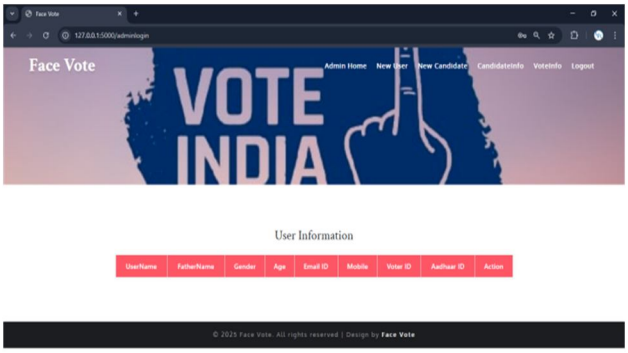


Figure 5: Admin Dashboard - Voter Information

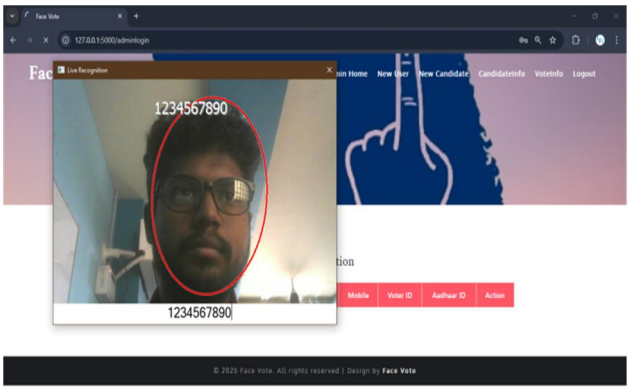


Figure 6: Real-Time face detection for voter Authentication

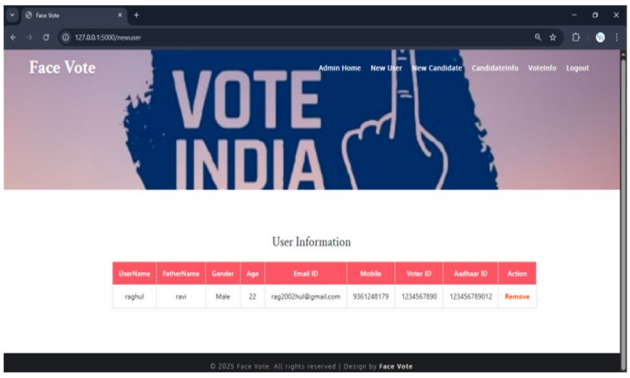


Figure 7: Registered voter information Table

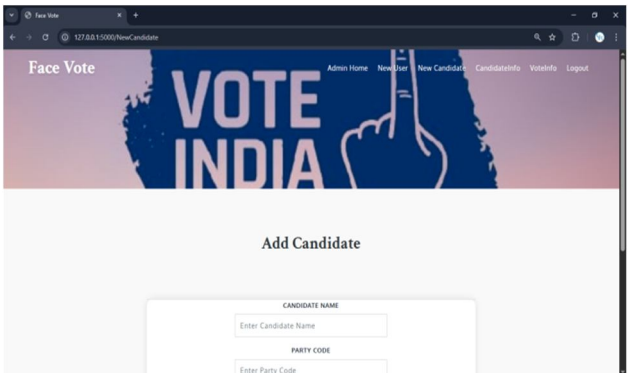


Figure 8: Add new candidate - registration form

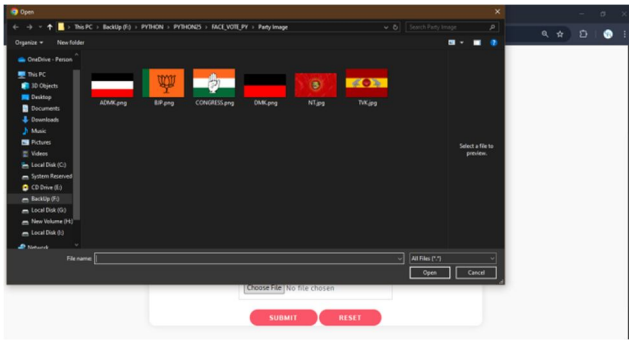


Figure 9: Party Symbol & candidate list

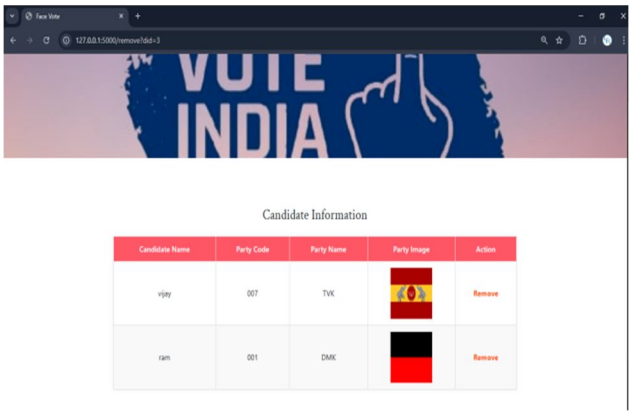


Figure 10: Candidate information List(DB)

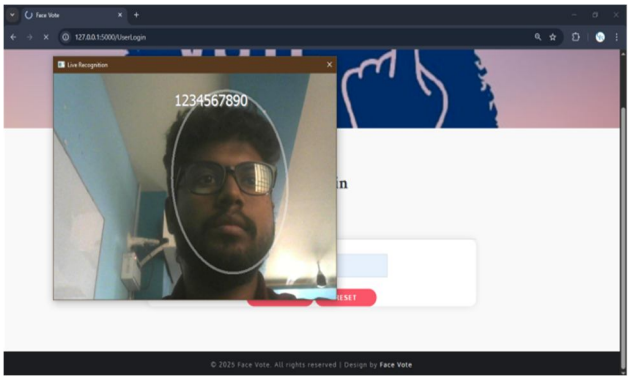


Figure 11: Face matching for secure vote access

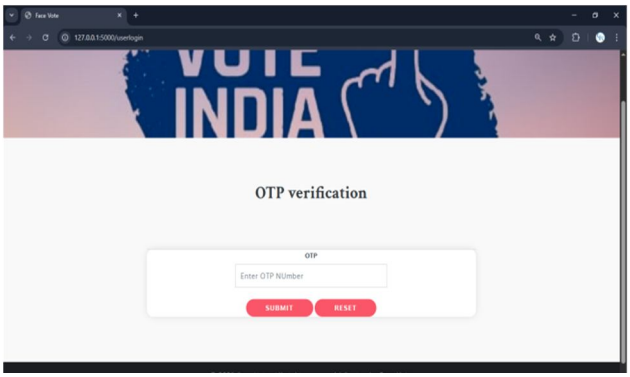


Figure 12: OTP verification for voter login authentication

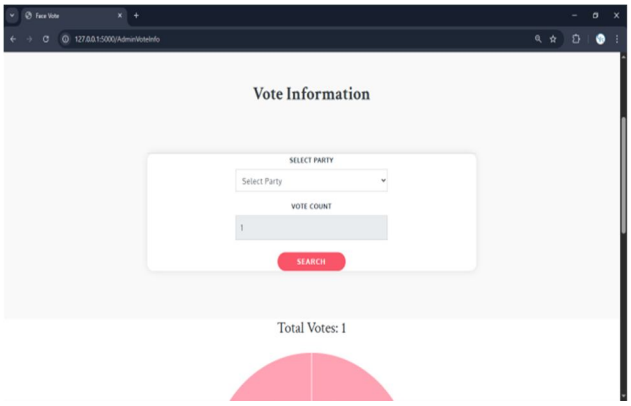


Figure 13: Live voting portal: party selection and vote casting

IX. CONCLUSION

From this discussion, it is evident that the proposed Vote Ledger system is a viable solution to modern day electronic voting by combining biometrics with blockchain technology. Facial recognition, which uses the Grassmann algorithm, ensures that voter verification is done accurately, making sure that only those who qualify get to vote while keeping impersonation and other security risks at bay. The use of blockchain technology adds to the effectiveness of the system as all transactions made during an election are stored safely and can never be altered. In addition, the system guarantees voter anonymity and privacy alongside end-to-end verification using unique transaction IDs that are sent through secure channels of communication. The results (fig 3 to 13) of experimentation showed high levels of accuracy, robust data integrity, speedier transaction processes, and timely results. As opposed to the traditional models of e-voting, the new system provides a higher degree of trust, accountability, and resistance to any form of cyber attacks and centralized failures. The decentralized system minimizes the reliance on the election officials while ensuring transparency during the voting process. Moreover, the voting platform facilitates the management of the elections while supporting scalability and mass adoption. Overall, the project shows that integrating biometrics with blockchain technology is highly effective in the modernization of the existing electoral systems.

X. FUTURE WORK

Some future prospects regarding the scope of this project could involve using more cutting-edge technology in order to improve the security, scale, accessibility, and user-friendliness of the Vote Ledger. Further developments could involve the inclusion of additional biometrics such as fingerprint scanning, iris recognition, or even voice recognition in addition to face recognition for improved voter identification purposes. Future versions of the system could be scaled up to include national and even international elections involving distributed blockchain networks with millions of transactions being executed per second. Blockchain algorithms that use minimal computing resources for increased efficiency might also become a part of the project. Other technological advancements which could potentially be included would include using artificial intelligence algorithms for detecting any potential cases of fraud and analyzing unusual voting behavior. Technologies like zero knowledge proofs and homomorphic encryption can also be combined to enhance privacy while retaining transparency.

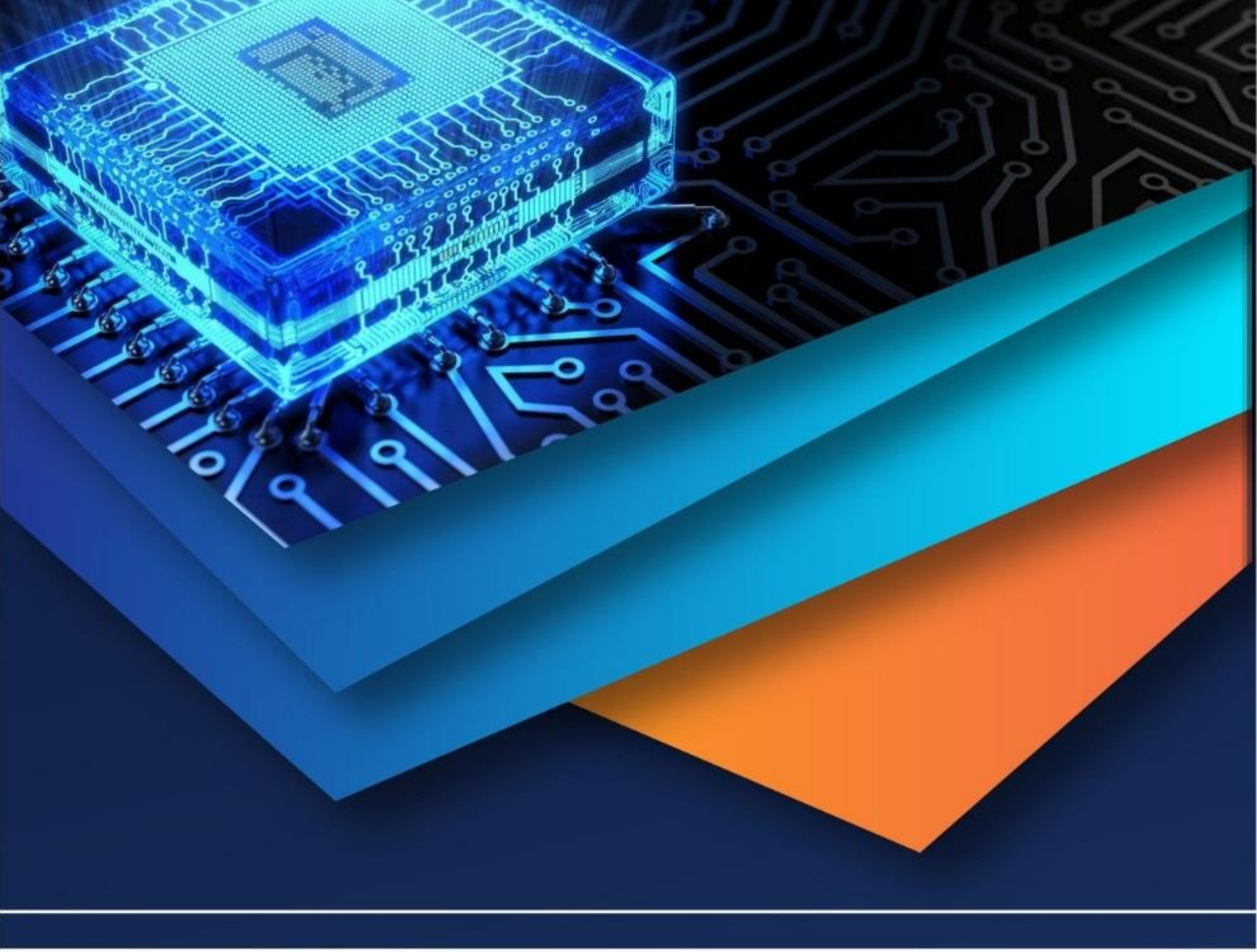
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The smart contract functionality can be enhanced to include features for automatic dispute resolution, scheduling of elections, and rules management. Cloud-based and edge computing infrastructure can help improve availability and speed. The integration of government databases of voters' identification can help automate the process of voter verification and registration. Legal compliance components and audit analytics dashboards can also be built into the system for use by the election officials. In summary, the future potential of this project can be seen in the development of an intelligent and globally applicable digital voting solution that will revolutionize democratic elections.

REFERENCES

[1] Kho, Yun-Xing, Swee-Huay Heng, and Ji-Jian Chin. "A review of cryptographic electronic voting." Symmetry 14.5 (2022): 858.
[2] HajianBerenjestanaki, Mohammad, et al. "Blockchain-based e-voting systems: a technology review." Electronics 13.1 (2023): 17.
[3] Burka, Dávid, et al. "Voting: A machine learning approach." European Journal of Operational Research 299.3 (2022): 1003-1017.
[4] Benabdallah, Ali, et al. "Analysis of blockchain solutions for E-voting: a systematic literature review." IEEE Access 10 (2022): 70746-70759.
[5] Goldberg, Mitchell, and Fabian Schär. "Metaverse governance: An empirical analysis of voting within Decentralized Autonomous Organizations." Journal of Business Research 160 (2023): 113764.
[6] Rathee, Geetanjali, et al. "On the design and implementation of a blockchain enabled e-voting application within iot-oriented smart cities." IEEE Access 9 (2021): 34165-34176.
[7] Alvi, SyadaTasmia, et al. "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system." Journal of King Saud University-Computer and Information Sciences 34.9 (2022): 6855-6871.
[8] Faruk, Md Jobair Hossain, et al. "Bie vote: A biometric identification enabled blockchain-based secure and transparent voting framework." 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA). IEEE, 2022.
[9] Vladucu, Maria-Victoria, et al. "E-voting meets blockchain: A survey." IEEE Access 11 (2023): 23293-23308.
[10] Varaprasada Rao, K., and Sandeep Kumar Panda. "Secure electronic voting (E-voting) system based on blockchain on various platforms." Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2. Singapore: Springer Nature Singapore, 2022. 143-151.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



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)