International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

A Decentralized Biometric Voting Framework using Grassmann Subspace Verification

Ashika Shereen M Bavani P Dharshini S Logasri A Dr.I.Shahanaz Begum
M.I.E.T. Engineering College College, Trichy-Pudukottai Road Affiliated Anna University (Autonomous),
ashikashereen@gmail.com bavaniammu1436@gmail.com dharshiii.sd@gmail.com
logasri502@gmail.com shahanazbegum.i@miet.edu

https://doi.org/10.55041/ijsmt.v2i4.180

Cite this Article: M, A. S., S, D., A, L. & P, B. (2026). A Decentralized Biometric Voting Framework using Grassmann Subspace Verification. International Journal of Science, Strategic Management and Technology, *02*(04). https://doi.org/10.55041/ijsmt.v2i4.180

Abstract— Electronic voting systems are increasingly adopted; however, they suffer from critical issues such as voter impersonation, vote manipulation, and lack of transparency. This paper proposes a secure e-voting framework that integrates real-time facial recognition with Grassmann subspace-based verification to achieve accurate and reliable voter authentication. Furthermore, a blockchain-based architecture utilizing SHA-256 is employed to ensure secure and immutable vote storage. The proposed system performs live facial data acquisition during both the registration and voting phases to enable continuous identity verification and prevent unauthorized access. Each vote is transformed into a unique cryptographic hash and stored within a blockchain ledger, ensuring data integrity, non-repudiation, and resistance to tampering or duplication. Experimental evaluation indicates that the proposed framework significantly enhances authentication accuracy, system security, and transparency when compared to conventional voting mechanisms.

Keywords— E-Voting, Face Recognition-Grassmann Manifold, Blockchain SHA-256, Biometric Authentication**.**

I. INTRODUCTION

Electronic voting (e-voting) systems have significantly transformed traditional voting processes by enhancing efficiency, reducing human intervention, and enabling faster result computation. Despite these advantages, existing e-voting systems remain susceptible to several critical security challenges, including identity fraud, vote manipulation, and risks associated with centralized data storage. Identity fraud allows unauthorized individuals to cast votes, while data tampering can compromise the integrity of election results. Furthermore, centralized architectures introduce single points of failure, making the system vulnerable to cyberattacks and unauthorized access.

Biometric authentication techniques, such as fingerprint and facial recognition, have been introduced to strengthen voter identity verification. Although these methods improve authentication accuracy, standalone biometric systems are still vulnerable to spoofing attacks, where fake biometric inputs (such as images or replicas) can deceive the system. Therefore, relying solely on biometric authentication is not sufficient for ensuring complete security. To address these limitations, blockchain technology has emerged as a promising solution by providing decentralization, transparency, and immutability. In a blockchain-based system, data is distributed across multiple nodes, eliminating centralized control and reducing the risk of data breaches. Additionally, the use of cryptographic mechanisms such as SHA-256 ensures that once a vote is recorded, it cannot be altered or deleted, thereby maintaining data integrity and trust.In this context, the proposed system introduces a hybrid framework that integrates real-time facial recognition with Grassmann subspace verification for robust and continuous voter authentication. The incorporation of Grassmann manifold-based techniques enhances the accuracy of facial recognition by effectively handling variations in pose, illumination, and facial expressions. Furthermore, the integration of blockchain-based secure storage ensures that all votes are recorded in a tamper-proof and transparent manner. This combined approach not only strengthens authentication

but also guarantees secure and reliable vote management, making the system suitable for real-world deployment.

A. Advantages of Blockchain Based E-Voting

• **Security:** The cryptography used in blockchain technology, along with SHA-256, prevents unauthorized access and data modification. In addition, live face recognition combined with OTP authentication provides multi-factor security, ensuring that only legitimate voters can access the system.

• **Transparency:** All votes are recorded on a blockchain ledger, allowing real-time verification while maintaining voter privacy and trust.

• **Efficiency:** The voting and counting processes are automated, enabling faster result declaration since all operations are performed in real time.

• **Accessibility:** The system allows users to vote from anywhere. With **OTP-based verification and facial authentication**, voters such as military personnel, overseas citizens, and physically challenged individuals can securely participate.

• **Cost-effectiveness:** The system reduces the need for physical infrastructure, polling staff, and paper-based processes, leading to significant cost savings.

B. Enhancing Voter Participation

The proposed e-voting system improves voter participation by enabling secure remote voting through blockchain technology. By using real-time facial recognition along with OTP authentication, it ensures that only valid voters can access the system. This allows people living away from their native place, such as students and employees, to vote easily. It also supports overseas citizens and physically challenged individuals. As a result, the system increases overall voter turnout while maintaining security and reliability. Significance of E-Voting System

The blockchain technology has potential to revolutionize the overall voting system. It will make the democratic beliefs stronger which is the foundation for the significance of decentralized and automated online voting systems. These systems' main benefits include:

Increased transparency: All the transactions in a blockchain system can be publicly available for verification which makes the system more transparent that traditional system

Increased security: Since blockchain uses cryptographic methods there is no room for anyone being able to alter the records in the voting system. Unauthorized people cannot access the system.

Building trust: There is no need to worry about the integrity of election since each vote is counted transparently, and all the votes are counted without any inaccuracy.

Increased availability and inclusivity: This technology enable accessibility from anywhere so anyone can vote. The military personnels, citizens overseas and physically disabled people can also cast vote.

Auditability and responsibility: Since every vote is recorded on a blockchain, there is a consistent audit trail that can be reviewed to ensure the accuracy of the election results.

Speed and efficiency: Real-time voting is made possible by blockchain, which shortens wait times and speeds up the election process overall.

II. LITERATURE REVIEW

In recent years, blockchain technology has gained significant attention in electronic voting systems due to its ability to provide transparency, security, and immutability. Many researchers have proposed various blockchain-based e-voting models to overcome the limitations of traditional and electronic voting systems. However, each approach has its own strengths and limitations.

Ashwani Kumar Pandey et al. (2024) proposed a blockchain-based framework titled *"Establishing Trust in Online Voting: Blockchain Solutions for Secure Elections with Immutability and Efficiency"*. This study focuses on improving trust in online elections by utilizing blockchain technology. The system ensures immutability of voting data and enhances efficiency in election management. It also enables secure vote handling and faster result processing. However, the system does not deeply integrate biometric identity verification, which may limit its effectiveness in preventing unauthorized voting.

Harshith Singathala et al. (2024) introduced a *"Blockchain Based E-Voting System"* that utilizes cryptographic techniques to securely store and verify votes. The proposed model ensures data integrity and prevents vote manipulation through decentralized architecture. While the system provides strong security and reliability, it lacks advanced voter authentication methods and provides limited discussion on scalability, which may affect performance in large-scale elections.

Kushal C. S. et al. (2025) proposed a system titled *"Design and Implementation of a Blockchain-Based Secure and Transparent Electronic Voting System"*. This approach emphasizes transparency and tamper resistance by recording votes as blockchain transactions. The system improves trust in the voting process by ensuring that data cannot be altered.

However, the model mainly focuses on vote storage security and does not fully address advanced biometric authentication, leaving potential gaps in voter identity verification.

Dhruv Kumar Maurya et al. (2025) developed an *"E-Voting System Based on Blockchain"* that introduces a decentralized voting framework to eliminate centralized control. The system enhances vote integrity and ensures secure vote transmission and storage. Although decentralization reduces the risk of centralized attacks, the system lacks real-time fraud detection mechanisms and does not sufficiently address biometric authentication challenges.

Hamza Baniata et al. (2025) proposed *"BP-Vot: Blockchain-Based e-Voting Using Smart Contracts, Differential Privacy, and Self-Sovereign Identities"*. This system focuses on privacy preservation by integrating advanced techniques such as smart contracts and differential privacy. It also introduces self-sovereign identity concepts to protect voter data. While the system provides strong privacy and identity control, it involves higher computational complexity and implementation challenges, which may limit its practical deployment.

A. Comparative Analysis and Research Gap

From the above literature, it is observed that most blockchain-based e-voting systems successfully address issues such as data security, transparency, immutability, and decentralization. However, several common limitations still exist across these models.

Most systems lack robust biometric authentication mechanisms, which are essential for ensuring that only authorized voters participate in elections. Additionally, some systems do not provide real-time fraud detection and rely heavily on secure data storage rather than complete voter validation. Scalability and implementation complexity are also major concerns in certain approaches.

B. Objective of the Proposed System

To overcome the limitations identified in existing systems, the proposed work aims to develop a **secure, transparent, and efficient blockchain-based electronic voting system**. The system integrates advanced authentication techniques such as **live face recognition and OTP-based verification** to ensure accurate voter identity validation and prevent unauthorized access.

By leveraging blockchain technology, the proposed system ensures **data immutability, transparency, and tamper resistance**, while the added authentication layers enhance the overall security of the voting process. This combination helps in minimizing fraud, eliminating duplicate voting, and increasing trust among users.

Furthermore, the system is designed to provide **reliability, scalability, and ease of use**, making it suitable for real-world implementation. It can be effectively applied in various domains such as **educational institutions, organizational elections, and large-scale public elections**, thereby creating a **secure, transparent, and trustworthy voting environment**.

III. METHODOLOGY

The proposed system follows a structured methodology to ensure secure and reliable online voting using facial recognition and cryptographic techniques. The workflow consists of multiple stages, including user registration, authentication, vote casting, and secure data storage. The design of this system is inspired by existing blockchain-based voting frameworks **[1]– [5]**.

Initially, the **user registration process** is carried out where the voter provides personal details such as name, age, email, mobile number, voter ID, and Aadhaar ID. During this stage, the system captures the user's facial data using a camera. The captured image is pre-processed through face detection, alignment, and normalization to improve accuracy. The processed facial features are then stored securely in the database for future authentication. The use of biometric authentication enhances voter verification as discussed in prior systems **[2], [4]**.

During the **login phase**, the user enters their voter ID. The system retrieves the corresponding user details from the database and initiates the facial recognition process. A live image is captured and compared with the stored facial data using a recognition algorithm. If the face matches successfully, the user is allowed to proceed; otherwise, access is denied, ensuring that only authorized individuals can vote. This approach improves identity validation beyond traditional methods used in earlier blockchain voting systems **[1], [3]**.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

After successful face verification, the system performs an additional layer of security using **One-Time Password (OTP) verification**. An OTP is generated and validated to confirm the user's identity. Multi-factor authentication improves system reliability compared to existing models that lack strong voter validation **[2], [5]**.

Once authentication is completed, the user is directed to the **voting interface**, where a list of candidates is displayed. The user selects their preferred candidate and submits the vote.

To ensure data integrity, each vote is stored using cryptographic hashing (SHA-256), similar to blockchain-based storage techniques discussed in previous studies **[1], [3], [5]**.

The system checks whether the user has already voted by verifying the voter ID in the database, thereby enforcing the rule of "one person, one vote."

To ensure data integrity and prevent tampering, the system uses **cryptographic hashing (HMAC with SHA-256)**.

Each vote is stored along with a unique hash value generated using a combination of voter ID, selected party, timestamp, and the previous hash value. This creates a chain-like structure similar to blockchain, making it extremely difficult to alter any recorded vote without detection.

Finally, the **admin module** allows authorized personnel to monitor the system, manage users and candidates, and view voting results. The system calculates total votes, displays vote distribution using graphical representations, and identifies the winning candidate based on the highest number of votes.

This methodology ensures a secure, transparent, and efficient voting process by integrating biometric authentication, multi-level security, and blockchain-inspired data protection techniques.

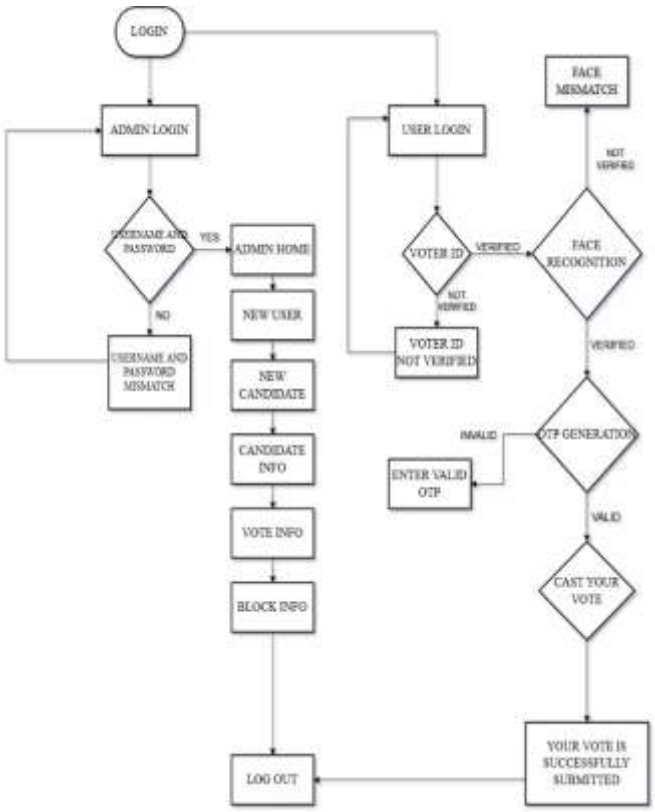

Fig. 1. Flowchart

IV. RESULTS

The proposed Face Recognition-Based Online Voting System was successfully implemented and tested under various conditions to evaluate its performance, accuracy, and security compared to existing blockchain-based voting models [1]– [5].

The system demonstrated reliable functionality across all modules, including user registration, authentication, voting, and result analysis.

During the registration phase, user details along with facial data were captured and stored in the database without errors. The face recognition module effectively verified users by comparing live facial input with stored data, ensuring that only authorized voters could access the system. In cases of mismatch, the system correctly denied access, thereby preventing unauthorized voting.

The integration of OTP verification added an additional layer of security. Only users who successfully completed both face recognition and OTP validation were allowed to proceed to the voting stage. This multi-level authentication significantly reduced the risk of identity fraud.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **04** April-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

The **voting module** functioned accurately by allowing each registered user to vote only once. The system successfully prevented duplicate voting by checking the voter ID against existing records in the database. Upon casting a vote, the system stored the vote securely along with a unique hash value generated using SHA-256, ensuring data integrity.

The implementation of **blockchain-inspired hashing** proved effective in maintaining tamper-proof records. Each vote was linked with a previous hash value, forming a secure chain that prevents unauthorized modifications.

The **admin module** provided a clear overview of voting activities, including total votes, party-wise vote counts, and winner identification. The results were displayed using graphical representation (pie chart), which improved readability and analysis.
Overall, the system achieved:

- Accurate user authentication
- Secure and tamper-proof vote storage
- Prevention of duplicate voting
- Efficient vote counting and result generation

The experimental results confirm that the proposed system is reliable, secure, and suitable for modern digital voting applications.

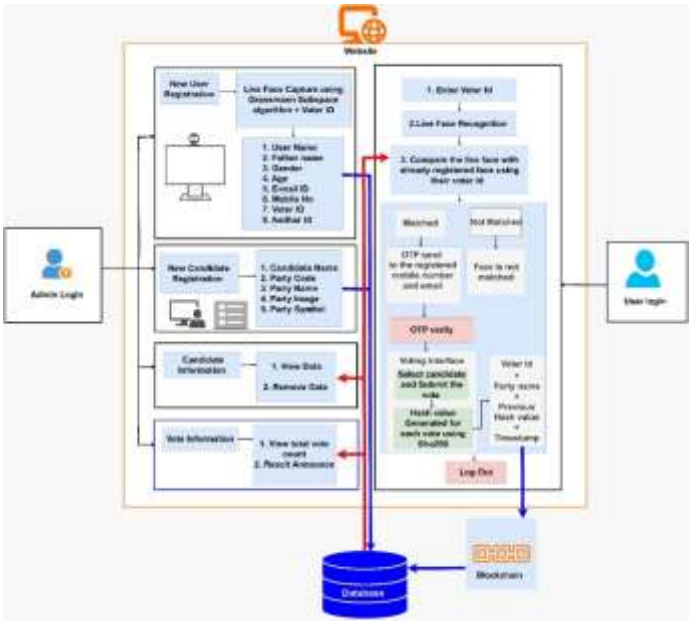

Fig.2 Architecture

Fig.3 Live Face Recognition

Fig.4 Voting interface

V.CONCLUSION

The **Face Recognition-Based Online Voting System** was successfully designed and implemented to provide a secure, efficient, and transparent voting platform. The system integrates advanced technologies such as facial recognition, OTP verification, and cryptographic hashing to ensure strong user authentication and data security.
The use of **biometric verification** ensures that only legitimate users can access the system, while OTP authentication adds an additional layer of protection against unauthorized access. The implementation of **SHA-256 hashing** provides data integrity by making the voting records tamper-proof and secure.
The system effectively enforces the principle of **"one person, one vote"**, preventing duplicate voting and ensuring fairness in the election process. Additionally, the admin module enables easy

monitoring of voting activities and provides clear result visualization through graphical representation. Overall, the project demonstrates that integrating biometric authentication with secure data handling techniques can significantly improve the reliability and transparency of online voting systems. This approach can serve as a foundation for developing more advanced and scalable e-voting solutions in the future.

VI.REFERENCES

[1] A. K. Pandey, et al., "Establishing Trust in Online Voting: Blockchain Solutions for Secure Elections with Immutability and Efficiency," *IEEE Conference/Journal*, 2024.
[2] H. Singathala, et al., "Blockchain-Based E-Voting System," *IEEE Conference/Journal*, 2024.
[3] K. C. S., et al., "Design and Implementation of a Blockchain-Based Secure and Transparent Electronic Voting System," *IEEE Conference/Journal*, 2025.
[4] D. K. Maurya, et al., "E-Voting System Based on Blockchain," *IEEE Conference/Journal*, 2025.
[5] H. Baniata, et al., "BP-Vot: Blockchain-Based E-Voting Using Smart Contracts, Differential Privacy, and Self-Sovereign Identities," *IEEE Conference/Journal*, 2025.