INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

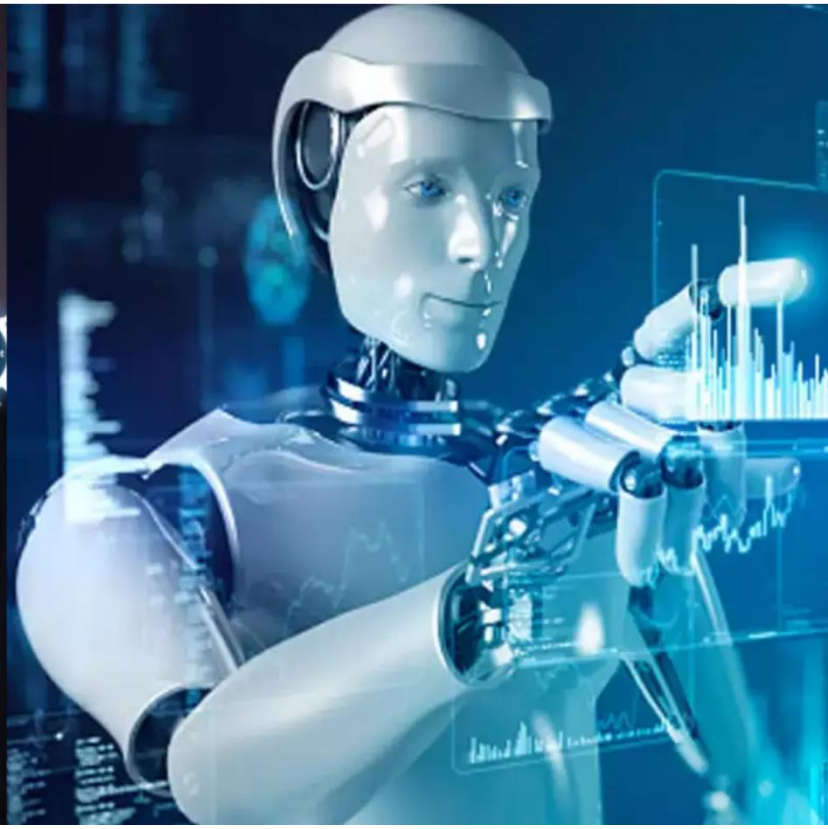
Scan to save the contact details

IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503382|

E-Voting With Facial Recognition and Blockchain

S. Venu Gopal [1], Rayala Charanya[2], Ramavath Swamy[3], Suryawanshi Steevan[4]

Assistant Professor, Department of Information Technology, ACE Engineering College, Hyderabad, Telangana, India[1]

IV B.Tech Students, Department of Information Technology, ACE Engineering College, Hyderabad, Telangana, India [2, 3, 4]

ABSTRACT: Voting is an important part of any democratic system, but traditional methods still face problems such as fake voting, manual errors, and lack of transparency. This paper presents a secure e-voting system using facial recognition, OTP verification, and blockchain technology. The system authenticates voters using facial recognition and OTP, ensuring that only authorized users can vote. Each vote is encrypted and stored in a blockchain, preventing any modification. The proposed system improves security, reduces fraud, and provides faster and more transparent results compared to existing voting methods, making it suitable for modern digital elections

KEYWORDS: E-Voting, Blockchain, Facial Recognition, OTP, Multi-Factor Authentication, Security

I. INTRODUCTION

Elections play a key role in maintaining democracy, and ensuring fair voting is very important. Traditional voting systems such as paper ballots and Electronic Voting Machines (EVMs) still face several issues like impersonation, vote tampering, long queues, and delays in counting results. These problems reduce trust among people.With the development of technology, online voting systems have been introduced. However, many of these systems are not fully secure, as they depend on simple authentication methods and centralized databases, making them vulnerable to hacking and manipulation.To overcome these challenges, this paper proposes a secure e-voting system using facial recognition, OTP verification, and blockchain technology. This approach ensures strong authentication and tamper-proof vote storage, improving security, transparency, and reliability.

II. LITERATURE SURVEY

Recent studies on e-voting systems highlight the use of blockchain technology to improve security and transparency. A study titled *"Blockchain-Based Electronic Voting System"* by M. Tariq et al. (2020) proposes a decentralized framework where votes are stored in an immutable ledger. This approach ensures transparency and prevents vote tampering. However, the system lacks strong biometric authentication, making it vulnerable to impersonation since it does not verify the actual identity of voters.Another work, *"Secure E-Voting Using Blockchain"* by A. Singh et al. (2022), focuses on secure vote storage and traceability using blockchain technology. It eliminates dependence on centralized authorities and enhances trust in the voting process. Despite these advantages, the system does not include biometric verification such as facial recognition and lacks real-time fraud detection, making it less effective against unauthorized access.

Research on biometric-based systems, such as *"Biometric Voting System Using Machine Learning"* by S. Ahmed et al. (2021), introduces machine learning techniques for voter authentication. This method improves identity verification compared to traditional approaches. However, it faces issues with scalability and performance when handling large datasets and does not provide secure vote storage, as blockchain integration is not included.Overall, existing systems either focus on blockchain for secure vote storage or biometrics for authentication, but fail to provide a complete solution. The proposed system addresses these gaps by integrating facial recognition, OTP verification, and blockchain technology, ensuring secure, reliable, and scalable e-voting.

III. METHODOLOGY

The proposed system is designed to provide a secure and transparent electronic voting process by integrating multi-factor authentication, facial recognition, and blockchain technology.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503382|

System Architecture:
The system consists of modules including registration, authentication, voting interface, and blockchain storage. These components work together to ensure secure communication, reliable identity verification, and tamper-proof vote storage.

Registration:
In this phase, the user registers by entering personal details and capturing facial data using a camera. The system processes the captured image using FaceNet and MediaPipe models to extract facial features. To protect user privacy, the extracted data is converted into a secure format using the SHA-256 hashing algorithm. This ensures that sensitive personal and biometric data are not stored in raw form.

Authentication:
During login, the system verifies the identity of the voter using a two-step authentication process. First, a One-Time Password (OTP) is sent to the user's registered mobile number via call. The user must enter the correct OTP for initial verification. After successful OTP verification, facial recognition is performed using FaceNet and MediaPipe by comparing the live image with the stored facial data. This process ensures accurate and secure user authentication while preventing unauthorized access.

Voting:
After successful authentication, the voter accesses the voting interface and selects a candidate. The selected vote is encrypted before being processed further, ensuring confidentiality during transmission.

Blockchain Storage:
The encrypted vote is stored as a transaction in the blockchain. Each block contains the vote data, timestamp, and the hash of the previous block. The SHA-256 algorithm is used to generate a unique hash for each block, ensuring immutability and security. Any attempt to modify stored data will change the hash value, making tampering easily detectable.

Data Flow:
1. User registers and facial data is captured.
2. FaceNet and MediaPipe extract facial features.
3. SHA-256 generates secure hash for user data.
4. User logs in and receives OTP via call.
5. OTP is verified, followed by facial recognition.
6. User casts vote through the interface.
7. Encrypted vote is stored in blockchain with hash linkage.
8. System maintains a secure and tamper-proof voting record

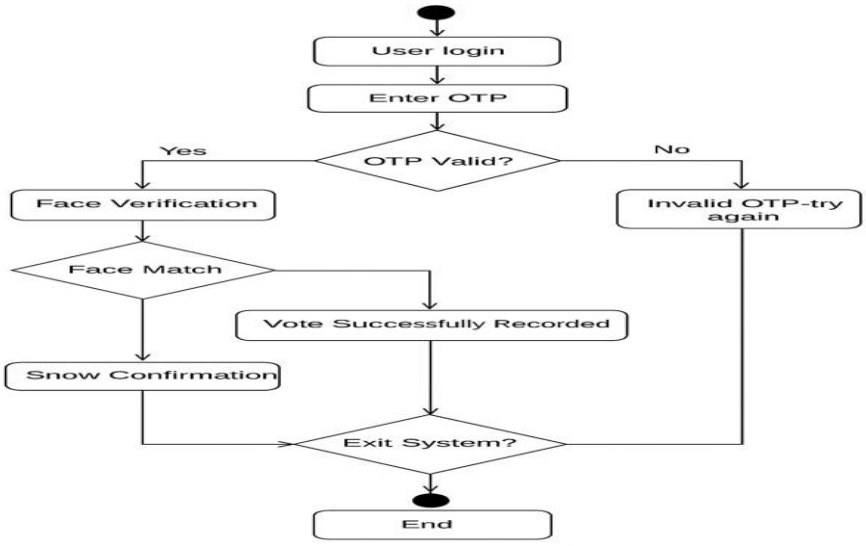


Fig 3.1 E-voting System Methodology

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503382|

IV. SYSTEM ARCHITECTURE

The *Phone Buddy - Offline Remote Device Control* system is designed to provide secure and efficient offline remote control of smartphones through SMS communication. The process begins when a user sends a command from a trusted mobile number, which is received by the SMS Receiver module in the application. The message is then forwarded to the authentication module, where the sender's number and passcode are verified to ensure that only authorized users can access the system.

Once validated, the command is passed to the command processing module, which identifies the requested action. The system controller then executes the appropriate operation, such as locking the device, changing ringer modes, retrieving contacts, or sending location details.

The SQLite database is used to store trusted numbers, passcodes, and other necessary data. After execution, the SMS Manager generates a response and sends it back to the user. This architecture ensures reliable, secure, and smooth functioning even without internet connectivity.

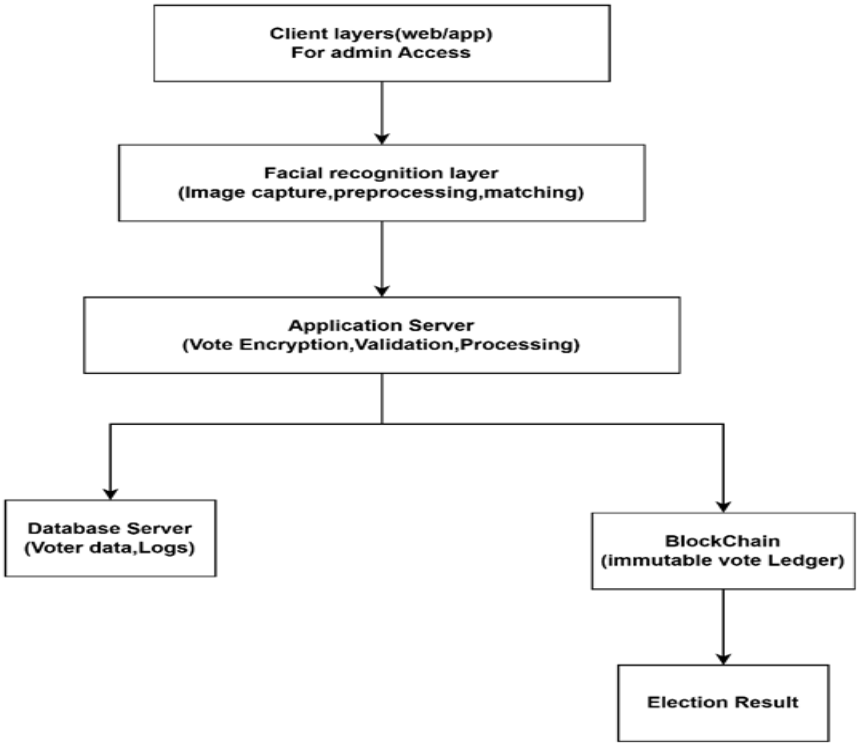


Fig 4.1 System Architecture

V. RESULTS

The proposed E-Voting system was evaluated to analyze its performance, security, and reliability. The system successfully integrates OTP-based authentication, facial recognition, and blockchain technology to ensure secure voting. The authentication process using OTP and facial recognition achieved accurate identity verification with an average response time of approximately 3–4 seconds. The system effectively prevented unauthorized access and ensured that only valid users could participate in voting. The blockchain module provided secure and immutable storage of votes. Each vote was encrypted and stored using SHA-256 hashing, ensuring that data cannot be altered or tampered with. The system also prevented duplicate voting, ensuring one vote per user. Compared to traditional voting systems, the proposed system demonstrates improved security, transparency, and efficiency.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503382|

Table 5.1 Comparison with Existing Systems

Feature	Existing System	Proposed System
Authentication	Manual/Password	OTP + Facial Recognition
Security	Low	High
Vote Storage	Centralized	Blockchain
Transparency	Medium	High
Fraud Risk	High	Low

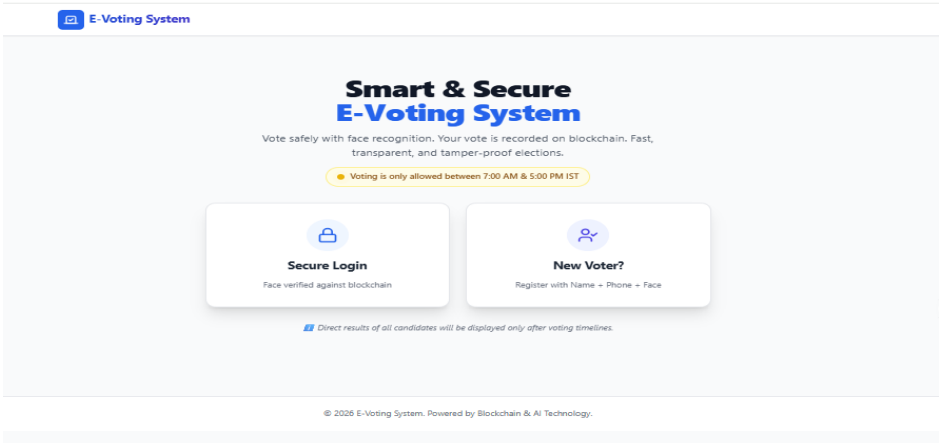


Fig 5.1

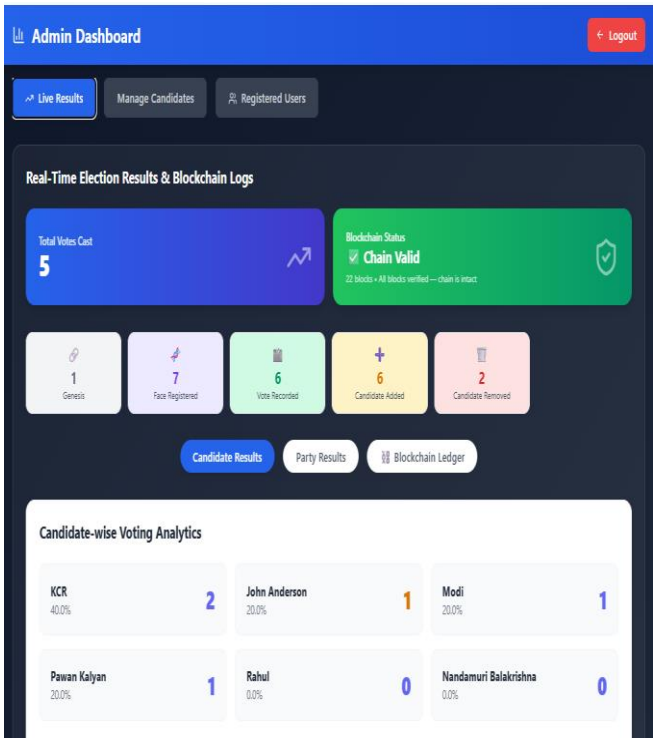


Fig 5.2

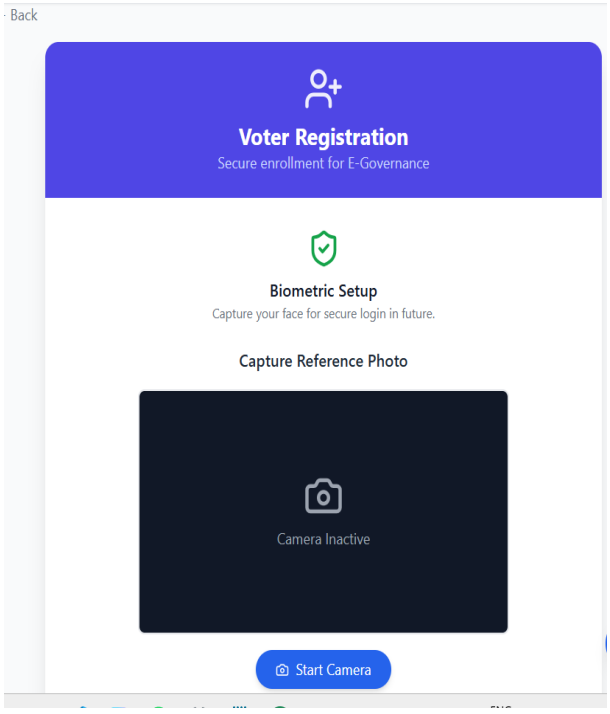


Fig 5.3

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503382|

Fig 5.4

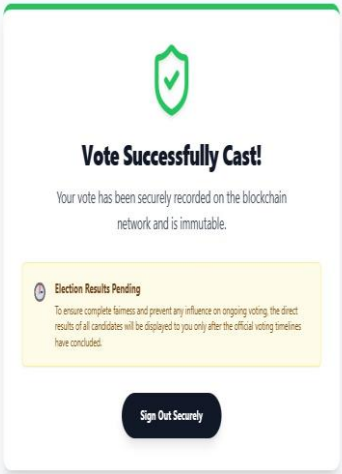


Fig 5.5

VI. CONCLUSION

The proposed E-Voting system successfully demonstrates a secure and reliable digital voting solution by integrating facial recognition, OTP-based authentication, and blockchain technology. The system ensures accurate voter identification and prevents unauthorized access through multi-factor authentication. The use of SHA-256 hashing and blockchain technology guarantees data integrity and immutability, making the voting process tamper-proof and transparent. The system also eliminates issues such as duplicate voting, impersonation, and delays in result processing. Overall, the proposed approach improves security, efficiency, and trust in the voting process, making it suitable for modern digital election systems.

VII. FUTURE SCOPE

The E-Voting system can be enhanced by integrating advanced technologies and improving scalability. It can adopt real blockchain platforms like Ethereum for better security and decentralization, along with advanced AI models for accurate face recognition and fraud detection. Adding multi-factor authentication, including biometric and Aadhaar-based verification, will strengthen security.

The system can be scaled for national-level elections using cloud deployment and microservices architecture. A mobile application can improve accessibility and user experience, while multilingual support ensures wider usability.

Further improvements include real-time analytics, audit trails, and advanced encryption techniques like homomorphic encryption to enhance transparency and data privacy. Regular security updates, testing, and compliance with legal standards will ensure reliability and practical adoption.

REFERENCES

[1] A. Parmar et al., *"Secure E-Voting System using Blockchain Technology and Authentication via Face Recognition and Mobile OTP,"* IEEE, 2021.
Available: https://ieeexplore.ieee.org/document/9580147
[2] Mukherjee, A., Majumdar, S., Kolya, A. K., & Nandi, S. (2023). A privacy-preserving blockchain-based e-voting system. arXiv preprint, arXiv:2307.08412. https://arxiv.org/abs/2307.08412
[3] Russo, A., Fernández Anta, A., González Vasco, M. I., & Romano, S. P. (2021). Chirotonia: A scalable and secure e-voting framework based on blockchains and linkable ring signatures. arXiv preprint, arXiv:2111.02257. https://arxiv.org/abs/2111.02257
[4] Ahmed, S., et al., "Bie Vote: Biometric Identification Enabled Blockchain-Based Voting Framework," International

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503382|

Journal of Advanced Computer Science and Applications (IJACSA), 2021.
[5] Fan, Y., et al., "A Blockchain-Based Identity Management System for E-Voting," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10603–10614, 2021.
[6] Khan, L. U., et al., "AI and Blockchain for Next-Generation E-Voting Systems," IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1573–1602, 2022.
[7] Sharma, R., et al., "AI-Based E-Voting Authentication System Using CNN and MediaPipe," IEEE CINE Conference, 2022.