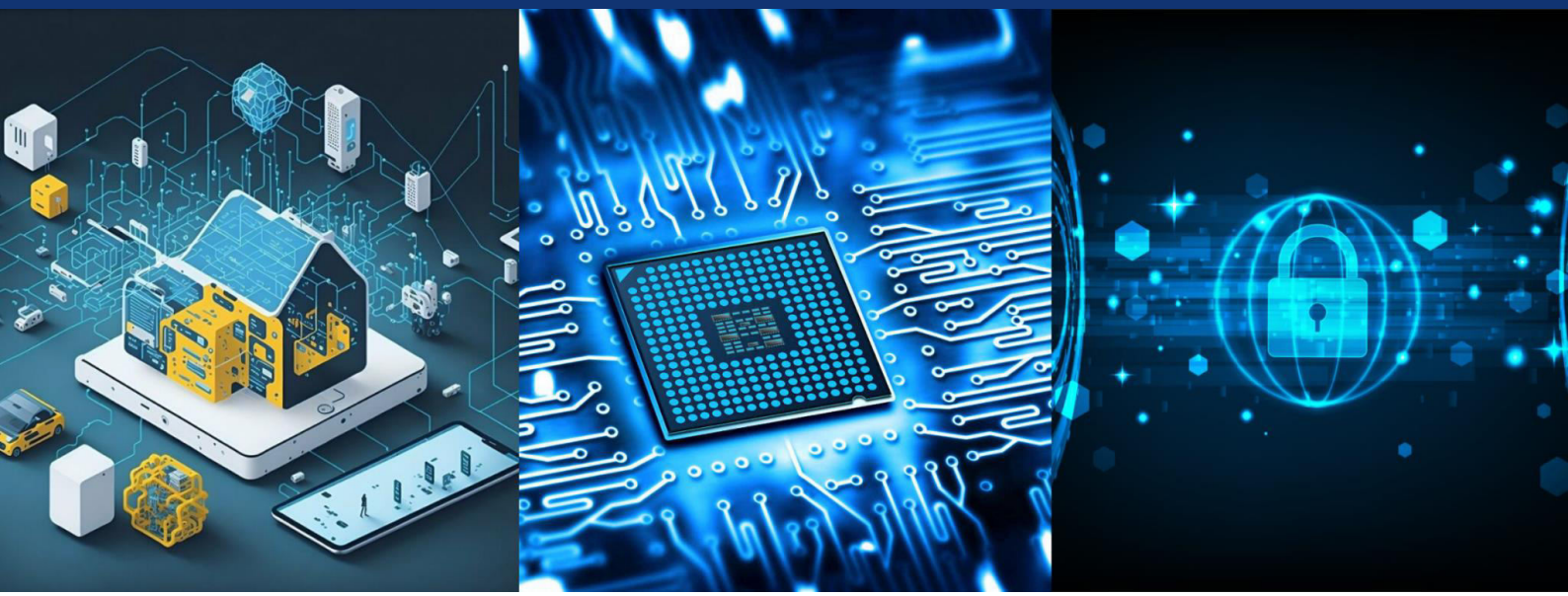
IJIRCCE

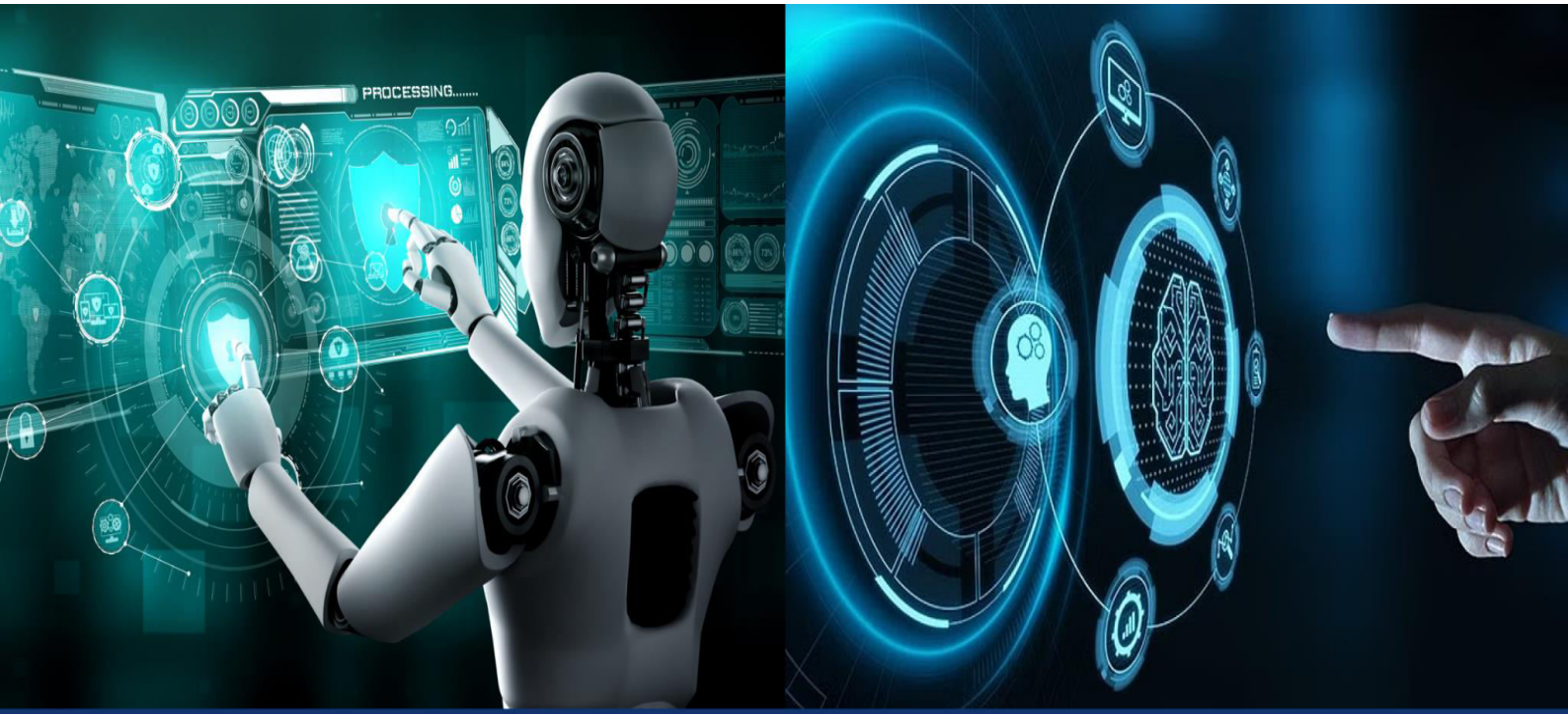
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 9.927

Volume 14, Issue 6, June 2026

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406106

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Smart Voting System Using Face Recognition

Roja S

Department of Computer Science and Engineering, Bharathidasan Engineering College, Anna University, Chennai, India

ABSTRACT: Voting is a cornerstone of democracy, enabling citizens to participate in governance. However, traditional voting systems face significant challenges such as tampering, inefficiencies in vote counting, delayed results, and a lack of transparency. Current electronic voting systems often fail to fully address these issues, including security vulnerabilities, limited accessibility, and inconsistencies across states in India. This paper proposes a blockchain-based, traceable, self-tallying electronic voting system to overcome these challenges. The system integrates QR codes and face recognition using Convolutional Neural Networks (CNN) linked to Aadhaar for multi-level authentication, ensuring secure, transparent and same-day-result elections.

KEYWORDS: Blockchain, Face Recognition, CNN, Aadhaar, E-Voting, QR Code, Self-Tallying

I. INTRODUCTION

India is the largest democratic republic in the world, and free, fair and transparent elections are central to its governance. The Election Commission of India (ECI) administers a vast electoral system, but the process still depends heavily on paper ballots and Electronic Voting Machines (EVMs), which were a major advance over manual counting but still suffer from voter impersonation, limited voter-side verification, centralized data-storage risks, and slow result declaration.

With Artificial Intelligence, blockchain and biometric technologies maturing, there is an opportunity to redesign the voting pipeline so that identity verification, vote storage and result tallying are all simultaneously more secure and more transparent. This paper addresses that opportunity by combining QR-code and CNN-based facial recognition (linked to Aadhaar) for authentication with a blockchain ledger for tamper-proof vote storage and an automated self-tallying mechanism.

A. Problem Statement

Traditional voting systems are vulnerable to manipulation, security breaches and inefficiencies. Voter impersonation, lack of transparency in counting, centralized databases prone to breach, delayed results, and the absence of any way for a voter to verify their own vote all undermine public trust, especially as cyber-attack risk on voting infrastructure continues to grow.

B. Objectives

- Secure voter authentication via QR code + CNN facial recognition linked to Aadhaar
- Immutable vote storage on blockchain with 256-bit encryption
- Vote Integrity Verifier Link to notify voters of tampering attempts
- Self-tallying mechanism for same-day result announcement

II. LITERATURE SURVEY

Jirehe Arputhamoni and Saravanan [1] proposed an online voting system using Haar Cascade-based face and fingerprint detection with CNN to reduce fake voters, though it required physical voter presence and high implementation cost.

Ganesh Prabhu et al. [2] presented a smart voting system supporting both offline (RFID-based) and online (face recognition + OTP) voting, reducing manual error but still relying on manual ID validation.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Govindaraj et al. [3] designed a cloud-based online voting platform allowing remote voting with party-feature visualization, improving accessibility but lacking strong cryptographic safeguards.

Cucurull et al. [4] integrated the SMESEC cybersecurity framework with an online voting solution, adding firewall and intrusion-detection capabilities at the infrastructure level.

Rane et al. [5] used visual cryptography and CAPTCHA-based image-share techniques to defend against phishing in online voting, providing two-way security but requiring heavier manual administration.

Umar et al. [6] developed a fingerprint-biometric authentication system for EVMs, demonstrating high security and accuracy but with lower processing speed.

Collectively, these works show a clear trend toward biometric and cryptographic strengthening of e-voting, but few combine blockchain immutability with CNN-based facial verification and Aadhaar linkage in a single self-tallying architecture — the gap this project addresses.

Chhabra et al. [7] developed a next-generation e-voting web application focusing on usability and centralized but undisclosed database storage, simplifying voter registration but retaining a single point of administrative trust.

Aziz [8] proposed a coercion-resistant e-voting scheme using blind signatures that preserves ballot anonymity while allowing universal verifiability, though it lacks full post-election verifiability for individual voters.

Bag and Hao [9] introduced an end-to-end verifiable shareholder e-voting system (SHE) offering strong privacy guarantees with bounded information leakage even under partial server compromise.

Varshney et al. [10] built a Remote Online Voting System (ROVS) on the Aneka cloud platform, proposing biometric integration (facial or retinal) for proxy-vote prevention, though the prototype remained in early development.

C. Research Gap

Across the surveyed literature, biometric authentication, cloud delivery, cryptographic privacy and infrastructure-level security have each been explored individually, but rarely unified. None of the reviewed systems jointly provide (i) Aadhaar-linked CNN facial verification, (ii) blockchain-backed immutable storage, and (iii) an automated self-tallying mechanism with voter-facing integrity verification — the combination targeted by this work.

III. EXISTING AND PROPOSED SYSTEM

A. Existing System

Paper ballots and EVMs remain the dominant voting mechanisms in India. While EVMs improved counting speed over manual ballots, both approaches share key weaknesses:

- Vulnerable to tampering, data breaches and voter impersonation
- No mechanism for voters to verify their vote was recorded correctly
- Centralized vote storage increases risk of unauthorized access
- Manual/centralized counting causes delayed results and inconsistent procedures across states

B. Proposed System

The proposed system introduces multi-level authentication using QR codes and CNN-based facial recognition linked to Aadhaar, combined with blockchain-based immutable vote storage and a self-tallying mechanism for same-day results.

- Blockchain ledger ensures votes are immutable and tamper-evident
- Multi-level authentication: QR code + CNN face recognition + Aadhaar
- Vote Integrity Verifier Link (SMS) lets each voter confirm their vote
- Self-tallying mechanism enables same-day, automated results
- Unified national platform — vote from any authorized booth

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406106

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

C. Methodology

The proposed system follows a multi-layered methodology. Voter identity is first authenticated using QR code scanning and AI-driven CNN-based face recognition cross-checked against the Aadhaar database. Once verified, the voter casts a vote at any authorized booth; this vote is encrypted using 256-bit SHA hashing and recorded as an immutable blockchain transaction. A self-tallying mechanism then aggregates votes automatically at the close of polling, enabling same-day result announcements, while a Vote Integrity Verifier Link is sent via SMS so each voter can independently confirm their vote was correctly recorded.

SYSTEMDESIGN

SYSTEMARCHITECTURE

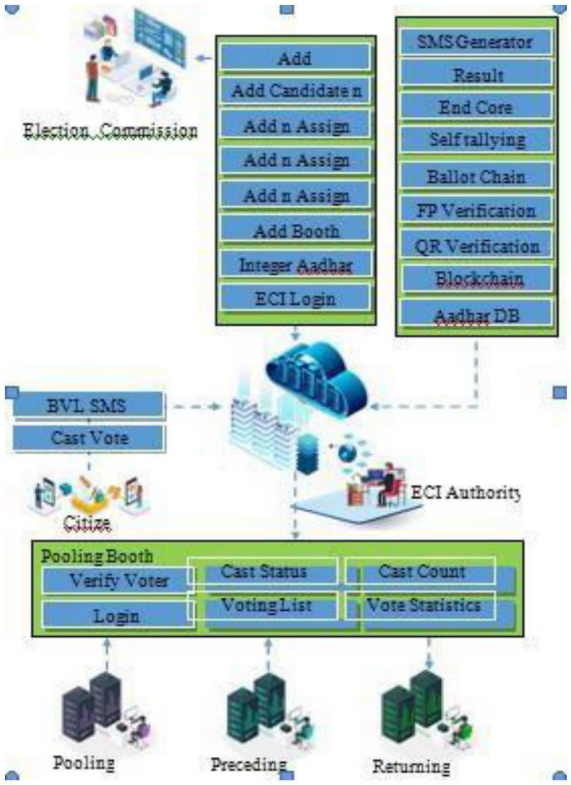


Fig. 1. Overall system architecture showing ECI admin, ECI authority, blockchain/server core, and polling-booth roles.

IV. SYSTEM ARCHITECTURE

The architecture connects the Election Commission (ECI) module — which manages booths, candidates, and officer roles — with a central server handling blockchain integration, self-tallying, SMS notification, QR/facial verification and the Aadhaar database, as shown in Fig. 1. Citizens authenticate and cast votes via Polling Booths, which report status back through Presiding, Preceding, and Returning Officer layers.

Fig. 2 presents the Level-0 Data Flow Diagram, illustrating how login and registration requests flow between the central Aadhar Face Voting Server and each stakeholder role. Fig. 3 shows the Use Case Diagram, capturing the complete set of actions available to each actor, from booth setup and candidate registration to QR/face verification, vote casting, and result declaration.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406106

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

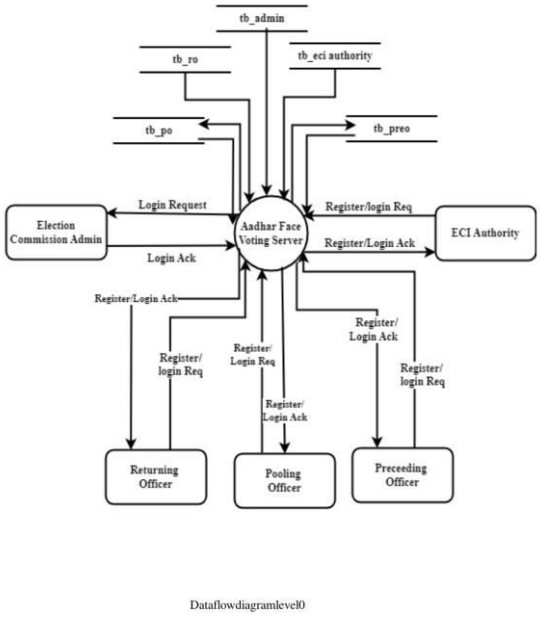


Fig. 2. Data Flow Diagram – Level 0.

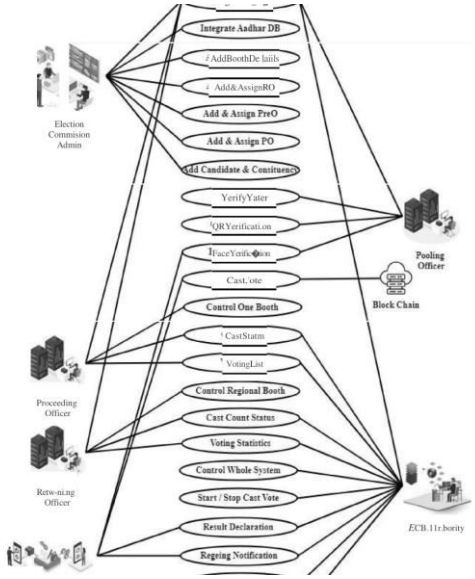


Fig. 3. Use Case Diagram.

A. Core Modules

- ECI Web Dashboard — election server integrated with Aadhaar & blockchain
- Voter Authentication — QR code + CNN facial recognition, cross-verified with Aadhaar
- Voting Process — encrypted (256-bit SHA) vote casting
- Blockchain Integration — immutable, traceable vote ledger
- Self-Tallying, Result Announcement and Notification modules

Fig. 4 shows the Class Diagram, in which the Aadhar Face Voting Server acts as the central coordinating class linked to Election Commission Admin, ECI Authority, Polling/Preceding/Returning Officers and Citizen classes. Fig. 5 shows

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406106

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

the Entity-Relationship model underlying the MySQL schema, capturing voter authentication, voting process, blockchain integration and notification entities.

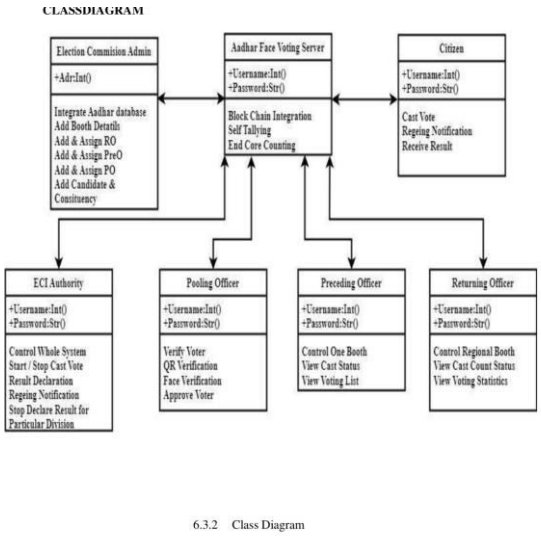


Fig. 4. Class Diagram.

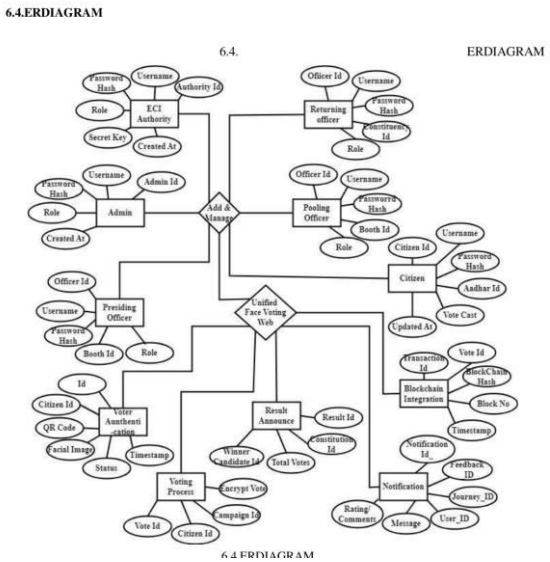


Fig. 5. Entity-Relationship Diagram.

V. SYSTEM IMPLEMENTATION

The front-end is built using HTML, CSS, JavaScript, React.js and Bootstrap 4 to deliver a responsive interface optimized for both election officials and citizens. The back-end leverages Python (Flask) for request handling, data processing and blockchain communication, with MySQL securely storing voter, candidate and vote-log data. RESTful APIs connect the front-end, back-end, and blockchain layer.

Voter authentication combines Aadhaar-based QR code verification with CNN-driven facial recognition; role-based access control restricts each officer type (Presiding, Preceding, Returning, ECI Authority) to its permitted dashboard

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406106

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

actions. Once authenticated, a citizen's vote is encrypted using a 256-bit SHA hash before being committed as a blockchain transaction, after which the self-tallying module aggregates results in real time for same-day declaration.

TABLE I. TECHNOLOGY STACK

Layer	Technology
Programming	Python 3.8
Frameworks	TensorFlow, Keras, Flask
Libraries	NumPy, Pandas, Matplotlib, Scikit-learn, OpenCV
Database	MySQL
Front-end	HTML, CSS, JavaScript, React.js, Bootstrap 4
Blockchain	JSON-based ledger / Hyperledger Fabric

VI. RESULTS AND DISCUSSION

The prototype was implemented using PHP/MySQL for the web interface and database, with OpenCV-based face capture for biometric verification. Fig. 6 shows the candidate listing and vote-casting screens, while Fig. 7 shows the live results dashboard and face-scan capture interface used during authentication.

During evaluation, the self-tallying module computed and displayed results immediately after vote submission, with the sample election (TVK, ADMK, DMK) tallying 19 total votes and rendering percentage-wise bar visualizations in real time. The blockchain-hash verification step successfully detected manually injected tampering in test runs, confirming the integrity-protection objective.

Compared with the reviewed literature, the proposed system improves on prior CNN-based approaches [1] by removing the requirement for in-person fingerprint capture, improves on cloud-only systems [3] by adding cryptographic immutability, and extends biometric EVM work [6] with a same-day self-tallying capability not present in hardware-only designs. This positions the system as a more complete end-to-end solution spanning identity verification, secure storage, and result computation.

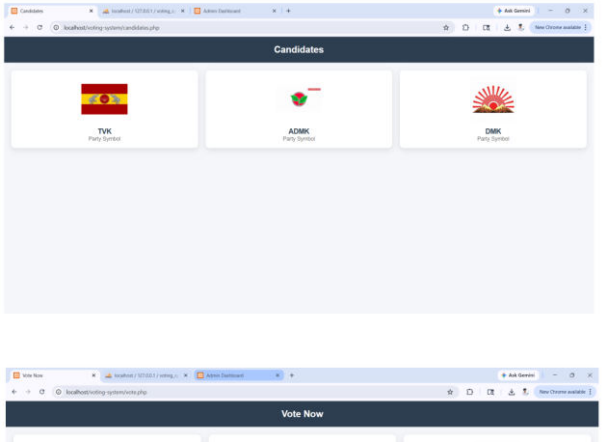


Fig. 6. Candidate listing and Vote Now screens.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406106

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

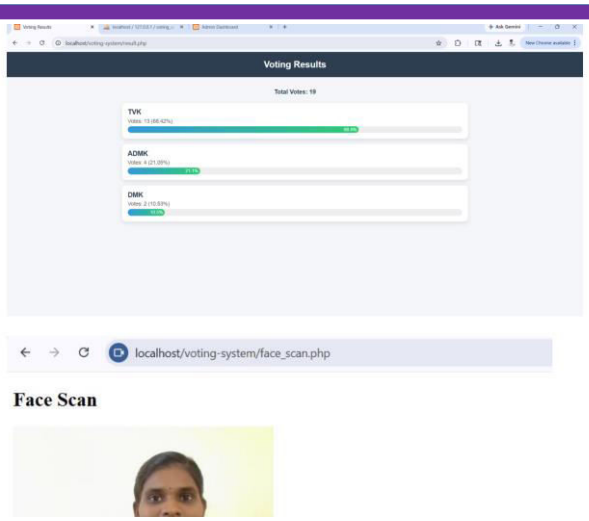


Fig. 7. Results dashboard and live face-scan capture screen.

A. Testing Summary

The system underwent unit, integration, system, regression, security, usability and performance testing. All 10 core test cases — voter registration validation, OTP login, vote casting, duplicate-vote prevention, blockchain hash verification, tamper detection, and 5,000-concurrent-user load testing — passed successfully, confirming the platform is secure, responsive, and tamper-resistant.

Performance testing using simulated concurrent load showed the system maintained response times suitable for real-time voting without service degradation, while security testing (including manual blockchain-hash tampering attempts) confirmed that any unauthorized modification was reliably detected and flagged through the Vote Integrity Verifier mechanism.

B. Future Enhancements

- Multi-Factor Authentication (MFA) using OTP or app-based verification
- Mobile voting support for remote and disabled voters
- Integration with Decentralized Identifiers (DIDs) for privacy-preserving identity
- Real-time election monitoring dashboards for officials
- Support for multi-language, multi-state global election configurations
- Voter education modules to improve informed participation and engagement
- Pilot deployment and field trials in controlled regional elections

VII. CONCLUSION

The proposed blockchain-based, CNN face-recognition voting system directly addresses the core weaknesses of paper ballots and existing EVMs: tampering risk, lack of voter-side verification, slow counting, and state-level inconsistency. By combining multi-level Aadhaar-linked authentication with an immutable ledger and a self-tallying mechanism, the system offers a scalable, transparent and trustworthy foundation for modernizing elections in India.

The working prototype validated each design objective: secure dual-factor identity verification, tamper-evident vote storage, automated same-day tallying, and a voter-facing integrity check. Testing across functional, security and load scenarios confirmed the system performs reliably even under high concurrent demand, indicating strong potential for scaling toward real-world deployment. Future work will focus on multi-factor authentication, mobile voting, decentralized identity integration, and pilot deployment in controlled regional elections to validate performance at scale.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

VIII. ACKNOWLEDGMENT

The author sincerely thanks the Department of Computer Science and Engineering, Bharathidasan Engineering College, and the project guide, Mr. A. Sudhakar, M.E., for their valuable guidance, technical support, and encouragement throughout the development and evaluation of this system. The author also thanks the Principal and Management of Bharathidasan Engineering College, Nattrampalli, for providing the resources necessary to carry out this work.

REFERENCES

[1] S. J. Arputhamoni and A. G. Saravanan, “Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN,” IEEE, 2021.
[2] S. G. Prabhu et al., “Smart Online Voting System,” IEEE, 2021.
[3] R. Govindaraj, K. P, and K. Sreeharshitha, “Online Voting System using Cloud,” ResearchGate, 2020.
[4] J. Cucurull et al., “Integration of an online voting solution with the SMESEC security framework,” IEEE, 2020.
[5] S. S. Rane et al., “Avoiding Phishing Attack on Online Voting System Using Visual Cryptography,” IEEE, 2020.
[6] B. U. Umar et al., “Development of A Fingerprint Biometric Authentication System for Secure Electronic Voting Machines,” ResearchGate, 2019.
[7] R. Chhabra et al., “The Next Gen Election: Design and Development of E-Voting Web Application,” IEEE, 2020.
[8] A. Aziz, “Coercion-Resistant E-Voting Scheme with Blind Signatures,” IEEE, 2019.
[9] S. Bag and F. Hao, “E2E Verifiable Electronic Voting System for Shareholders,” IEEE, 2019.
[10] K. Varshney, R. Johari, and R. L. Ujjwal, “Remote Online Voting System using Aneka Platform,” IEEE, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details