IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.151112

AI-Based Real-Time Duplicate Voter Detection Using Face Embeddings and Voice-Assisted Verification During Polling

Neha Nitin Wagh[1], Digvijaysing Devendra Rajput[2], Darshan Ranjeet Desale[3], Chetana Mukesh Sonawane[4], Dr. Nilesh Arun Patil[5]

UG student, SES's R. C. Patel Institute of Technology, Shirpur 425405 India[1-4]

Assistant Professor, SES's R. C. Patel Institute of Technology, Shirpur 425405 India[5]

Abstract: Artificial intelligence (AI) and biometric recognition technologies have created new possibilities for automated identity verification. However, applying these technologies in an election environment requires careful consideration of recognition errors, presentation attacks, data privacy, processing latency, and human accountability. This paper presents a proposed framework for real-time duplicate-voter screening during Election Day polling using facial recognition, a same-day voter registry, voice-assisted confirmation, and human-in-the-loop review.The proposed framework captures a facial image, generates or extracts facial features using the selected recognition method, and compares the observation against eligible records in the current-day registry.

Its proposed contribution is an end-to-end polling-day screening workflow that connects temporal registry search, multimodal evidence, uncertainty handling, and human review. No performance improvement is assumed without experimental evidence. The framework is intended as a research prototype and does not replace official electoral verification or authorized human decisions.[3]

1. INTRODUCTION

1.1 Background and Motivation

Identity verification is a fundamental requirement in systems where access, authorization, or service delivery depends on determining whether a person corresponds to a registered identity. Facial recognition has developed from classical image-description methods to deep-learning approaches that learn discriminative facial representations. Schroff et al. (2015), in *FaceNet: A Unified Embedding for Face Recognition and Clustering*, demonstrated an embedding-based approach in which facial images are represented as feature vectors suitable for comparison and clustering.[1] Despite advances in recognition methods, biometric matching is not error-free. Differences in illumination, facial pose, image quality, and the characteristics of the recognition model can affect matching performance.These findings reinforce the importance of measuring performance under relevant conditions rather than assuming that a model provides uniform accuracy for every population.Election-day verification introduces an additional operational requirement: identifying whether a person has already appeared in the relevant polling-day records.[10]

The proposed project addresses this problem through a workflow that searches the current-day registry for potential matches.The main motivation is therefore not to claim that facial recognition is a new technology, but to investigate whether integrating established biometric methods into a clearly defined polling-day process can support timely and accountable duplicate-candidate screening.[5]

1.2 Objectives of the Study

1. To develop a workflow for comparing a newly captured facial observation against records associated with the current polling day.
2. To investigate facial feature extraction and similarity matching using the recognition algorithm implemented in the prototype.
3. To examine the role of liveness assessment in reducing vulnerability to specified presentation attacks, where such a component is implemented.[6]
4. To distinguish voice-assisted name confirmation from actual speaker verification and evaluate the implemented function accordingly.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.151112

2. CONCEPTUAL FOUNDATIONS AND ENABLING TECHNOLOGIES

2.1 Facial Recognition and Feature Representation

Facial recognition involves extracting useful information from a facial image and comparing that information with stored reference data. Classical approaches, such as Local Binary Patterns Histograms (LBPH), describe local facial texture using histograms. Ahonen et al. (2006), in *Face Description with Local Binary Patterns: Application to Face Recognition*, demonstrated the use of local binary patterns for facial representation and recognition.[3]

Deep-learning approaches instead learn feature representations from large collections of facial images. Schroff et al. (2015) introduced FaceNet, which maps facial images into a compact embedding space designed to support recognition and clustering. In an embedding-based system, two facial observations can be compared using a distance or similarity measure. The comparison threshold determines which observations become candidate matches. 5]

2.2 Face Liveness and Presentation-Attack Detection

A facial recognition system may be vulnerable to presentation attacks in which an image, a replayed video, or another artificial representation is presented to the camera. Chingovska et al. (2012), in *On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing*, investigated texture-based approaches for distinguishing genuine facial presentations from spoofing attempts.[4]

The proposed workflow includes liveness assessment as a separate stage if supported by the implementation.The evaluation should specify the attack types tested, the number of trials, the failure conditions, and the measured error rates. If the current prototype does not implement liveness detection, this component must be identified as proposed future work rather than a completed feature.

2.3 Voice-Assisted Confirmation and Speaker Verification

Voice technologies can provide additional information during identity verification, but their functions must be distinguished. Speech-to-text converts spoken language into text, while speaker verification evaluates whether a voice sample corresponds to a claimed speaker. A spoken-name comparison therefore does not, by itself, establish the identity of the speaker.[4]

In the proposed framework, the polling officer may request a spoken name when a potential facial match is found. If the implementation uses speech-to-text, the recognized name can be compared with the name in the candidate record. The evaluation should measure speech-recognition errors and name-comparison errors. If speaker verification is implemented, genuine-speaker and impostor trials should be evaluated separately.[7]

2.4 Biometric Privacy and Template Protection

Facial images, voice recordings, and biometric feature representations create privacy and security risks when they are collected, stored, or processed without appropriate safeguards. Hahn and Marcel (2022), in *Biometric Template Protection for Neural-Network-Based Face Recognition Systems: A Survey of Methods and Evaluation Techniques*, examined techniques for protecting facial templates and discussed the need to evaluate recognition accuracy alongside properties such as irreversibility and unlinkability.

The research should document whether the implementation stores raw facial images, feature representations, audio, or only verification metadata. These storage choices have different privacy implications.The system should record the events necessary to understand the verification sequence while minimizing the exposure of sensitive information.[10]

3. RELATED WORK AND LITERATURE REVIEW

3.1 Review of Existing Research

Existing research provides a foundation for the individual technologies relevant to the proposed framework. Ahonen et al. (2006) investigated local binary patterns for facial description, while Schroff et al. (2015) introduced learned facial embeddings for recognition and clustering. These studies illustrate different approaches to representing faces and provide a basis for choosing an appropriate recognition component.For voice biometrics, Poddar et al. (2018) reviewed the challenges of speaker verification with short utterances.[8]

 This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJARCCE.2026.151112

3.2 Comparative Analysis of Existing Research

Sr. No.	Research / Approach	Technique Used	Advantages	Limitations
1	Ahonen et al. (2006)	Local Binary Patterns (LBP)	Extracts local facial texture features with relatively low computational complexity.	Performance can be affected by lighting conditions and image quality.
2	Schroff et al. (2015)	FaceNet facial embeddings	Represents faces as feature vectors for similarity comparison.	Requires appropriate threshold selection and suitable image quality.
3	Chingovska et al. (2012)	LBP-based face anti-spoofing	Studies texture-based methods for detecting facial presentation attacks.	May not reliably detect all types of presentation attacks.
4	Poddar et al. (2018)	Short-utterance speaker verification	Discusses challenges and methods for verifying speakers using short speech samples.	Background noise and short speech duration can affect reliability.
5	Grother et al. (2019)	Demographic effects in face recognition	Highlights the importance of evaluating demographic differences in recognition performance.	Evaluation findings do not directly establish the accuracy of a specific voter verification system.
6	Proposed System	Same-day registry search, facial matching, secondary identity confirmation, and manual review	Identifies potential duplicate records and provides a manual review process for uncertain cases.	Requires threshold calibration, privacy safeguards, and experimental validation.

3.3 Research Gap

The reviewed literature establishes that facial representation learning, presentation-attack detection, speaker verification, demographic evaluation, and biometric template protection have each been investigated extensively. The research gap for the present project should therefore not be framed as the absence of these technologies in existing research.[15]
Instead, the proposed study investigates their integration into a polling-day duplicate-screening workflow. The potential contribution lies in evaluating the entire operational sequence, including registry scoping, candidate matching, uncertainty handling, authorized review, and event logging. To establish novelty, the final study must identify and compare existing systems that address duplicate voter registration, biometric voter authentication, and election-day identity verification.[6]

4. PROPOSED SYSTEM ARCHITECTURE AND METHODOLOGY

4.1 System Architecture

The proposed framework consists of a facial capture module, a recognition component, a same-day registry search module, a secondary verification component, a decision-management layer, and an audit-log module. These components are connected through a defined verification workflow.The capture module receives the facial observation from a camera. The recognition component processes the image and generates a comparison result using the selected algorithm. The registry module searches records within the configured polling-day scope and retrieves a candidate record when a potential match is identified.[13]

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026
DOI: 10.17148/IJARCCE.2026.151112

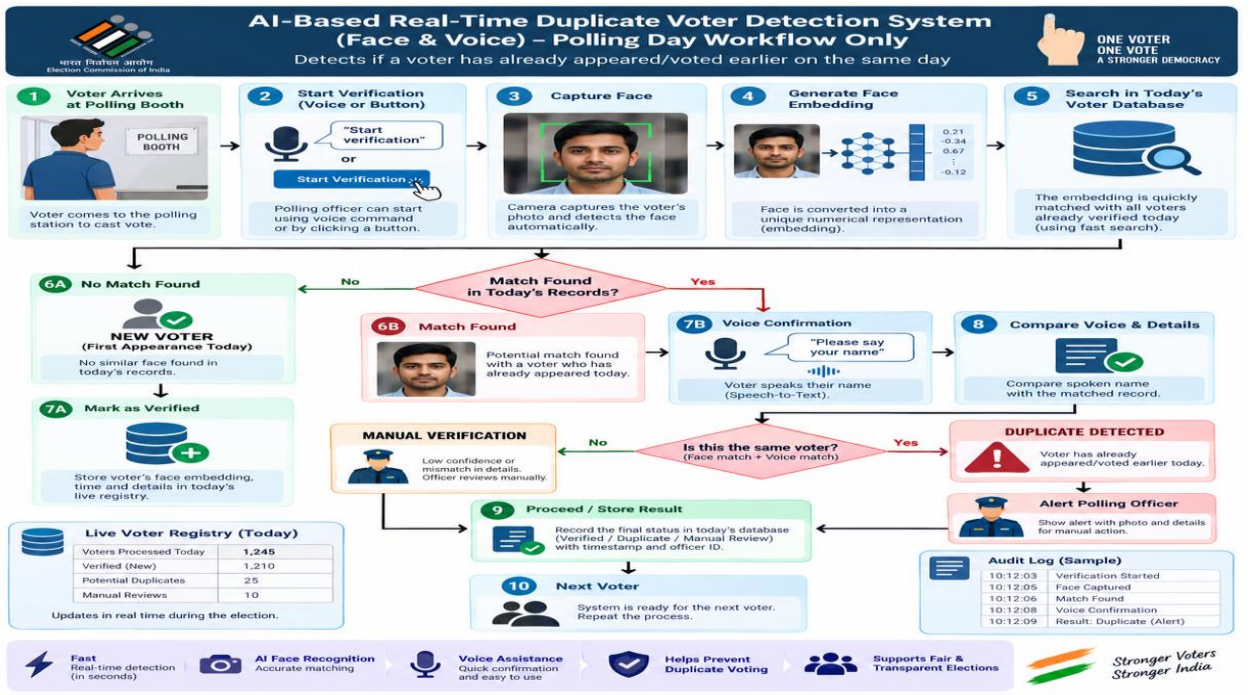


Figure 1. Proposed architecture of the polling-day duplicate-voter screening framework

4.2 Facial Matching and Registry Search

The facial matching stage processes a newly captured image and compares it with the permitted reference records in the current-day registry. For an embedding-based model, the comparison may use cosine similarity or Euclidean distance. For an LBPH implementation, the comparison follows the distance calculation supported by the selected recognizer. The system must not apply embedding-specific equations to an LBPH model without an appropriate explanation.[6]

The registry search returns a candidate only when the comparison meets the configured criterion. The outcome is recorded as either no potential match or a potential match requiring further verification. The system should also handle failed image capture, unavailable records, multiple similar candidates, and registry errors explicitly.The current-day restriction is an operational property of the search process. Its correctness should be tested by confirming that records from the wrong date or outside the permitted registry scope are not unintentionally included.[7]

4.3 Secondary Verification and Decision Management

When a potential facial match is identified, the system invokes the configured secondary verification stage. In a speech-to-text implementation, the spoken name is recognized and compared with the name associated with the candidate record. In a speaker-verification implementation, the voice sample is compared with an enrolled reference using the implemented model.The output of this stage is interpreted alongside the facial comparison.[2]

4.4 Proposed Algorithm

Input: Captured facial image, current-day registry, configured recognition threshold, and available secondary verification module.
Output: Verification status and audit event.

1. Initialize the verification session and record the timestamp.
2. Capture and validate the facial image.
3. Perform liveness detection, if implemented.
4. Extract facial features and compare them with current-day registry records.
5. If no potential match is found, proceed with official verification.
6. If a match is found, perform secondary verification.
7. Refer uncertain or conflicting cases for authorized manual review [2].
8. Log the verification outcome and reset the system for the next session.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.151112

5. EXPERIMENTAL EVALUATION AND DISCUSSION

5.1 Evaluation Strategy

The experimental study should compare the baseline face-only workflow with the extended verification workflow. Both configurations should be evaluated using the same appropriately authorized test cases and consistent ground-truth labels.[9]

The test dataset should include genuine repeated observations of the same identity, observations of different identities, and challenging cases such as poor lighting or low-quality captures where feasible. The dataset size, participant or sample selection method, capture conditions, and test protocol should be documented.The evaluation should report precision, recall, false-positive rate, false-negative rate, processing latency, and manual-review frequency. Liveness and voice-related components should be evaluated separately using metrics appropriate to their specific functions. The results should distinguish errors in facial matching from errors introduced by speech recognition, speaker verification, or the decision policy.[3]

5.2 Prototype Implementation and Output Results

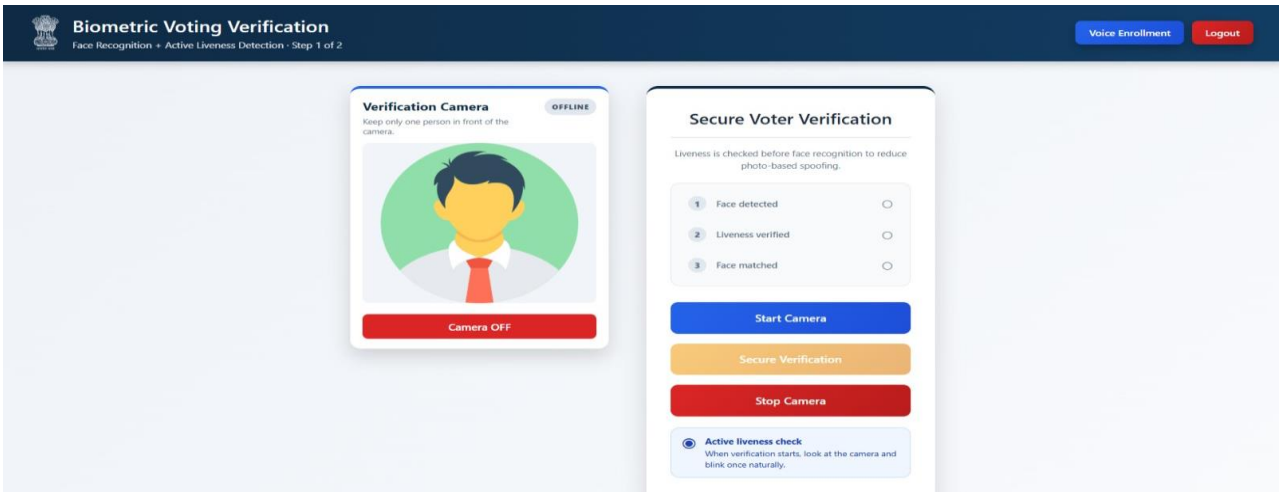


Fig. 2. Voter verification interface showing camera activation, verification controls, and facial registration proof.

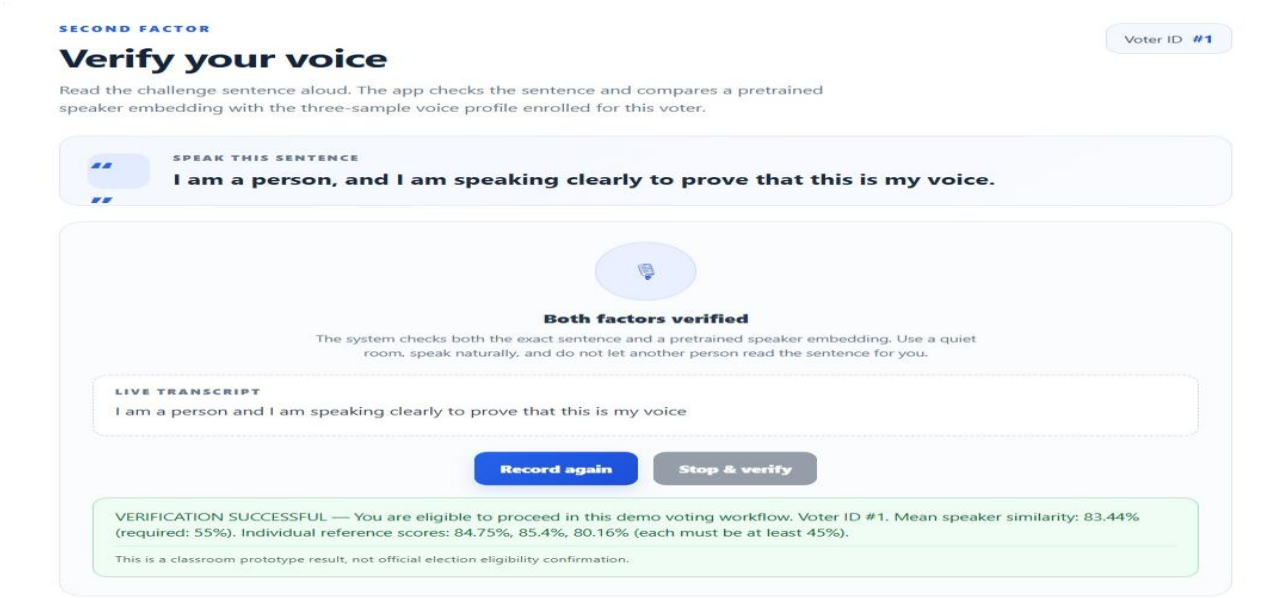


Fig. 3. Voice-Based Identity Confirmation Interface

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026

DOI: 10.17148/IJARCCE.2026.151112

5.3 Results Table

Sr. No.	Evaluation Metric	Illustrative Result
1	Total Test Samples	200
2	Correct Match Detection	45 out of 50 duplicate cases
3	Duplicate Detection Rate	90%
4	False Match Rate	5%
5	False Non-Match Rate	10%
6	Average Processing Time	1.5 seconds per verification
7	Cases Requiring Manual Review	15 out of 200 cases (7.5%)

Table 2. Illustrative Performance Evaluation of the Proposed System

5.3 Limitations

1. Face recognition accuracy may decrease under poor lighting conditions.
2. False matches and missed duplicates may occur.
3. Voice verification may be affected by background noise.
4. Biometric data requires strong privacy and security protection.

6. FUTURE RESEARCH DIRECTIONS

6.1 Improved Facial Recognition

Future research can compare classical LBPH recognition with embedding-based models such as FaceNet, where implementation resources and authorized data permit. The comparison should consider accuracy, false-match rates, latency, memory requirements, and performance under changes in lighting and facial pose. The objective is to identify a model appropriate to the operating conditions rather than assume that the most complex model will always perform best.[16]

6.2 Robust Liveness Detection

Future work can investigate presentation-attack detection using representative printed-photo, screen-replay, and other defined attack samples. The study can compare simple challenge-response techniques with texture-based or learned detection methods. The results should report which attacks are detected, which remain undetected, and the effect of the liveness stage on legitimate users and processing latency.[11]

6.3 Multimodal Verification

Further research can investigate whether combining facial evidence with a properly implemented voice-verification method improves the decision process. Speech-to-text-based name confirmation and speaker verification should be evaluated separately before investigating their combination with facial evidence. A controlled ablation study can estimate the contribution of each component and determine whether its benefit justifies its operational cost.[6]

CONCLUSION

This paper presents a proposed live voter registry-based framework for real-time duplicate-voter screening during Election Day polling. The framework integrates facial comparison with a same-day registry, a secondary verification stage, human review, and event logging. Its emphasis is on the operational workflow surrounding biometric matching rather than on claiming a new facial recognition algorithm.The proposed evaluation compares a face-only baseline with the extended workflow using recognition errors, processing latency, and manual-review workload.The system should be regarded as a research prototype until its performance, privacy safeguards, accessibility, and operational suitability have been appropriately validated.Ultimately, the research contribution will depend on whether the complete workflow provides measurable benefits under defined test conditions while preserving authorized human decision-making and protecting the rights of legitimate voters.

 This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJARCCE.2026.151112

REFERENCES

[1]. Devi, V. S., Kaavya, S., Deepika, B., Jayashree, D., & Nithikaa, L. (2026). AI-driven voter authentication and fraud detection system. *International Journal of Computer Technology and Electronics Communication*, *9*(3), 1008-1017.

[2]. Suhas, U., Matur, S. M., Farheen, Z., & Sultana, S. (2026, April). Sentinel: A Human-in-the-loop AI Framework for Electoral De-Duplication. In *2026 4th International Conference on Knowledge Engineering and Communication Systems (ICKECS)* (pp. 1-6). IEEE.

[3]. Kottur, S., Suresh, L. R., & Deepalakshmi, P. (2026, March). Enhancing Electoral Integrity Through AI-Powered Anomaly Detection and Blockchain Consensus. In *2026 International Conference on Data Science, Agents and Artificial Intelligence (ICDSAAI)* (Vol. 1, pp. 1-7). IEEE.

[4]. Calder, E. M. (2025). Responsible Use of AI in Electoral Roll Verification. *Journal of responsible AI & Ethics*, *2*(01), 82-99.

[5]. Reddy, G. M., Vijayalakshmi, V., & Usharani, S. (2026). AI-BASED ONLINE VOTING SYSTEM: INTEGRATING ISOLATION FOREST ANOMALY DETECTION, NLP SENTIMENT ANALYSIS, AND TF-IDF CANDIDATE MATCHING IN ASecure DJANGO ELECTORAL PLATFORM. *Journal of Informative & Futuristic Research (IJIFR)*, *13*(8), 1248-1256.

[6]. Ainur, J., Gulzhan, M., Amandos, T., Venera, R., Bulat, S., Zauresh, Y., & Aizhan, S. (2024). The impact of blockchain and artificial intelligence technologies in network security for e-voting. *International Journal of Electrical and Computer Engineering (IJECE)*, *14*(6), 6723-6733.

[7]. Sharma, H. (2025, October). Scalable Internet Voting Through AI-Driven Facial Recognition and Blockchain: A De-Duplication-Based Approach to Secure Voter Identity. In *2025 2nd International Conference on Computational Intelligence and Computing Applications (ICCICA)* (pp. 12-19). IEEE.

[8]. Ainur, J., Gulzhan, M., Amandos, T., Venera, R., Bulat, S., Zauresh, Y., & Aizhan, S. (2024). The impact of blockchain and artificial intelligence technologies in network security for e-voting. *International Journal of Electrical and Computer Engineering (IJECE)*, *14*(6), 6723-6733.

[9]. SarveshKrishna, A. K., Anbarasan, M., & Suguna, M. (2025, December). ECC-EXONUM-eVOTING: Enhancing Secure E-Voting with AI-Based Fraud Detection and Offline Voting Support. In *2025 Seventh International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 430-434). IEEE.

[10]. Srinivas, B., Maalini, D., Sudarshana, V., Sri Someshwari, M., Shopiga, E., & Saranya, M. (2025, April). Enhanced Electoral Voting System Using AI-Based Face and Iris Recognition
for Secure and Efficient Elections. In *2025 3rd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)* (pp. 1-6). IEEE.

[11]. Hayath, T. M., Rajeev, D. V., Nihanth, R., Tharun, U. V., & Achutha, R. (2026). Digital Voting System with Face Recognition. *International Journal of Scientific Research and Technology*, *3*(1).

[12]. Tahir, M., Khan, M. A. K. A., Faiz, S. F. S., & Muneeb, M. M. M. (2026). Securing Organizational E-Voting Through Blockchain, AES Encryption, Zero-Knowledge Proofs, and AI-Based Voter Authentication on Solana. *Pakistan Journal of Engineering, Technology and Science*, *14*(1), 83-98.

[13]. Pasha, X., & Jahankhani, H. (2024). Securing E-Voting Authentication: A Framework Integrating AI-Based Facial Recognition. In *Navigating the Intersection of Artificial Intelligence, Security, and Ethical Governance: Sentinels of Cyberspace* (pp. 19-46). Cham: Springer Nature Switzerland.

[14]. Pasha, X., & Jahankhani, H. (2024). Securing E-Voting Authentication: A Framework Integrating AI-Based Facial Recognition. In *Navigating the Intersection of Artificial Intelligence, Security, and Ethical Governance: Sentinels of Cyberspace* (pp. 19-46). Cham: Springer Nature Switzerland.

[15]. Gupta, K. R., Barthwal, A., Abdullah, M., & Rawat, A. S. (2026, May). A Survey Paper on Decentralized Blockchain-Based Voting System with AI-ML Based Behavioral Analysis. In *2026 IEEE 6th International Conference on Computing, Power, and Communication Technologies (IC2PCT)* (pp. 381-385). IEEE.

[16]. Muniru, A. N., & Sun, Q. (2026). AI based enhanced twofish encryption: empowering a secure voting mechanism with SnS and extended cyclic groups. *Cluster Computing*, *29*(1), 59.

[17]. Innocent, E., & Ojo, A. K. AI-Enhanced Decentralized Voter Accreditation using ERC-735: A Hybrid Blockchain Framework for Resource-Constrained Electoral Systems.

[18]. Gayathri, T., & Divya, J. S. (2025). A Comprehensive Review of Blockchain-Based E-Voting Systems: Security, Scalability, and Usability. *Algorithms in Advanced Artificial Intelligence*, 675-680.

[19]. Babu, B. R., Teja, J. R., Bhusan, T. S., Janardhan, A., & Thakur, A. (2023, February). Fpga based on voting system along with cross voters detection. In *2023 IEEE 3rd International Conference on Technology, Engineering, Management for Societal impact using Marketing, Entrepreneurship and Talent (TEMSMET)* (pp. 1-5). IEEE.



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 11, November 2026
DOI: 10.17148/IJARCCE.2026.151112

[20]. Shaikh, A., Adhikari, N., Nazir, A., Shah, A. S., Baig, S., & Al Shihi, H. (2025). Blockchain-enhanced electoral integrity: a robust model for secure digital voting systems in Oman. *F1000Research*, *14*, 223.
[21]. Shaikh, A., Adhikari, N., Nazir, A., Shah, A. S., Baig, S., & Al Shihi, H. (2025). Blockchain-enhanced electoral integrity: a robust model for secure digital voting systems in Oman. *F1000Research*, *14*, 223.
[22]. Treier, T., & Düüna, K. (2024). Identifying and solving a vulnerability in the estonian internet voting process: Subverting ballot integrity without detection. *IEEE Access*, *12*, 197766-197782.