IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

A Comprehensive Review on Secure Online Election Management Systems Using Facial Recognition Authentication

Ankush Pitambar Ahire[1], Suyog Dayanand Bhoite[2], Varsha Ramdas Hase[3], Karan Ravindra Dhatrak[4], Prof. Walke A. B.[5]
[1,2,3,4,5]Department of Computer Engineering
Vidya Niketan College of Engineering, Bota, Ahilyanagar (M.S) India

Abstract: *The growing reliance on digital platforms for governance has increased the demand for secure and transparent electronic voting systems. Traditional voting processes that depend on manual verification and paper ballots often face challenges such as impersonation, vote manipulation, and delayed result compilation. To overcome these issues, online election management systems have emerged as a modern alternative, offering convenience and efficiency. However, ensuring voter authenticity and preventing fraudulent activities remain major concerns. This paper presents a comprehensive review of secure online election management systems that incorporate facial recognition authentication. The study explores the integration of biometric verification with web-based voting architectures to enhance election security, reliability, and accessibility. It analyzes various existing approaches, focusing on system design, authentication techniques, data security, and user experience. The paper also highlights the role of Python-based frameworks, image processing algorithms, and encrypted databases in building robust e-voting environments. Through this review, an effort has been made to outline the advantages, limitations, and potential improvements of facial recognition–enabled election systems, emphasizing their importance in achieving fair and trustworthy digital elections.*

Keywords*:* Online Election Management, Facial Recognition, Biometric Authentication, Digital Voting, E-Governance

I. INTRODUCTION

Elections form the cornerstone of democratic governance, providing citizens with the right and responsibility to select their representatives and influence policy decisions [1]. The credibility of any democratic system depends largely on the transparency, security, and fairness of its election process. Traditional voting systems, which primarily rely on manual registration, paper ballots, and physical verification, often encounter significant challenges such as human errors, delayed counting, ballot tampering, and voter impersonation [2]. These issues not only hinder efficiency but also raise serious concerns regarding the integrity of electoral outcomes. As the digital era continues to evolve, there is an increasing demand for modernized election management systems that ensure both convenience and reliability without compromising security [3].

The shift towards online and electronic voting systems has been driven by the rapid advancements in information and communication technologies [4]. Online election systems aim to simplify the voting process by allowing eligible voters to cast their votes through secure digital platforms. However, the major challenge in such systems lies in authenticating the identity of voters and preventing unauthorized access [5]. Conventional username and password mechanisms are insufficient in high-stakes applications like elections, as they can be easily exploited through phishing attacks, credential theft, or brute-force techniques [6]. Consequently, integrating biometric authentication particularly facial recognition—has emerged as an effective strategy to enhance security, accountability, and voter confidence in online elections [7].

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

Facial recognition technology leverages the unique physiological features of an individual's face to verify identity with a high level of precision [8]. It operates by analyzing facial patterns, geometrical distances between features, and texture mappings that are nearly impossible to replicate or forge [9]. The incorporation of facial recognition in election systems not only strengthens voter authentication but also minimizes the possibility of multiple voting and impersonation [10]. In recent years, several studies have explored the integration of facial biometrics into e-voting frameworks using tools such as Python, OpenCV, and deep learning algorithms for real-time verification [11]. Such systems enhance both the security and convenience of the voting process, offering a seamless experience to users while maintaining data integrity [12].

In addition to authentication, data security and privacy remain fundamental concerns in digital elections [13]. The sensitive nature of voter data—including biometric information, credentials, and vote records—necessitates the implementation of encryption mechanisms, secure databases, and access control policies [14]. Modern frameworks like Flask and Django have been widely used for secure backend development, while SQLite and MySQL databases provide lightweight yet reliable storage solutions [15]. Furthermore, end-to-end encryption, hashing, and digital signatures are often implemented to ensure that votes cannot be intercepted or modified during transmission [16]. These techniques collectively contribute to maintaining the transparency and trustworthiness of the online election process [17].

Despite its advantages, the adoption of online election management systems faces several challenges, including concerns related to system scalability, network dependency, algorithmic bias, and voter privacy [18]. Facial recognition systems, though efficient, may occasionally encounter issues such as variations in lighting, pose, or image quality, leading to false rejections or acceptances [19]. Additionally, the ethical implications of storing biometric data raise questions about long-term privacy and data misuse [20]. Therefore, continuous research and technological refinement are essential to ensure that these systems achieve the desired level of reliability and inclusivity [21]. Governments, researchers, and software developers must work collaboratively to establish global standards and regulations governing digital election frameworks [22].

This paper presents a comprehensive review of secure online election management systems with an emphasis on facial recognition authentication. It explores various existing frameworks, technological architectures, and methodologies adopted in digital voting environments [23]. The study also discusses the advantages and limitations of current systems and highlights opportunities for future enhancement in areas such as deep learning integration, blockchain-based voting security, and cloud scalability [24]. Through this review, the paper aims to provide a clear understanding of how biometric and web-based technologies can jointly transform the future of electoral processes, making them more transparent, accessible, and tamper-proof [25].

II. PROBLEM STATEMENT

Traditional voting systems face several limitations, including manual errors, delayed result processing, and risks of voter impersonation, while existing online voting platforms remain vulnerable to identity theft and data breaches [26]. The absence of robust biometric authentication and secure data management mechanisms compromises election integrity and transparency [27]. Facial recognition technology offers a promising solution; however, challenges such as accuracy under varying conditions, data privacy, and secure integration within web-based frameworks persist [28]. Therefore, the problem addressed in this study is the need for a secure, efficient, and reliable online election management system that integrates facial recognition authentication to ensure voter legitimacy, prevent fraudulent activities, and maintain data confidentiality [29].

III. OBJECTIVE

- To design a secure online election management system integrating facial recognition for voter authentication.
- To ensure transparency, accuracy, and data confidentiality throughout the digital voting process.
- To develop a user-friendly interface for both voters and administrators using Flask and SQLite.
- To prevent fraudulent activities such as duplicate voting and unauthorized access.
- To evaluate system performance in terms of authentication accuracy, speed, and scalability.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

IV. LITERATURE SURVEY

[1] Rudra Pratap Singh et al. examined a web-based e-voting platform integrating facial recognition and OTP verification to prevent impersonation. Their research emphasized the dual-layer security approach, combining face biometrics with encrypted credential validation. They concluded that integrating real-time image matching significantly minimizes duplicate voting and enhances voter trust, though the system required optimization for large datasets.

[2] Mehta and Rao introduced an online election model using Python's OpenCV library and Haar Cascade classifiers for real-time face detection. Their model achieved high accuracy under ideal conditions but struggled with occlusion and poor lighting. The authors recommended adaptive thresholding and improved image preprocessing to address recognition errors in uncontrolled environments.

[3] Pacheco-Torgal and Jalali discussed secure digital identification frameworks applicable to e-governance, including electoral systems. Their study stressed the necessity of cryptographic protocols and decentralized storage to safeguard user identity and voting confidentiality. They suggested that incorporating blockchain or hash-based encryption enhances auditability and transparency in online elections.

[4] Patel and Singh analyzed different biometric techniques such as fingerprint, iris, and facial recognition for online verification. Their comparative evaluation found that facial recognition provides superior accessibility and speed for web-based voting, making it suitable for systems where voter convenience and scalability are key factors.

[5] Gupta et al. developed a CNN-based facial authentication system designed for secure logins in sensitive web applications. Their study demonstrated a 96% accuracy rate in face recognition under stable illumination and proposed the integration of cloud databases for scalable deployment in national elections.

[6] Sharma et al. explored multi-factor authentication models combining facial recognition with cryptographic key generation. Their findings revealed that the inclusion of dynamic encryption keys for every login session reduced spoofing attempts and ensured system integrity, providing a potential blueprint for high-security election platforms.

[7] Ahmed et al. designed a blockchain-integrated e-voting framework emphasizing immutability and voter anonymity. They proposed a decentralized ledger to store each vote as an encrypted block, preventing tampering and unauthorized modification. The system demonstrated reliability and transparency suitable for public-scale elections.

[8] Kaur and Bansal implemented a Flask-based web application that integrates facial recognition APIs with SQLite databases. Their system allowed seamless data exchange between the frontend and backend while maintaining lightweight performance. The authors highlighted Flask's modular architecture as a suitable framework for scalable election systems with real-time verification features.

[9] Choudhary et al. developed a security model for online elections using AES and SHA-256 encryption algorithms. Their approach ensured that votes and voter credentials remained protected throughout transmission and storage. They concluded that coupling biometric verification with advanced encryption provides the most effective security layer for digital voting.

[10] Deshmukh et al. conducted research on Local Binary Pattern Histogram (LBPH) techniques for robust facial feature extraction. Their experiments indicated that LBPH outperforms traditional recognition models under varying light conditions, making it ideal for voter verification environments where external factors may affect image quality.

V. PROPOSED SYSTEM

The proposed Online Election Management System with Facial Recognition Authentication is designed to provide a secure, transparent, and efficient platform for conducting digital elections. The system addresses the key limitations of traditional and existing online voting systems by integrating a dual-layered authentication mechanism—combining username-password verification with biometric facial recognition. This dual verification ensures that only legitimate users can cast their votes, thus maintaining election integrity and preventing impersonation or multiple voting attempts [10][14][19].

The system architecture consists of two major modules: the User Module and the Admin Module. The User Module facilitates registration, login, facial recognition-based authentication, and secure voting. During registration, users provide basic details and a facial image, which is processed and stored in the database as facial encodings using Python's face_recognition and OpenCV libraries. At the time of voting, the webcam captures a live image, which is

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

compared against the stored encoding. If a valid match is detected, the system grants access to the voting interface, allowing the user to select and submit their preferred candidate. Once the vote is cast, it is encrypted and stored securely in the SQLite database, ensuring tamper-proof record-keeping [11][16][21].

The Admin Module is responsible for managing the entire election process. Administrators can log in using secure credentials to access dashboards for voter management, candidate management, and real-time result tracking. Admins can also view analytical reports showing total votes per candidate and voter participation rates. Additionally, the system provides anomaly detection to flag suspicious activities, such as multiple login attempts or failed facial matches, thereby ensuring continuous monitoring and transparency [17][22][24].

Technologically, the proposed system uses Python Flask as the backend framework to handle server-side processing and routing between the user interface and the database. The frontend is developed using HTML, CSS, and JavaScript, ensuring a responsive and intuitive user experience. The SQLite database is used for data storage, maintaining user credentials, facial encodings, vote records, and candidate details. Data security is enforced through encryption, and strict validation checks are implemented to prevent SQL injection and data leakage. The integration of OpenCV and facial recognition libraries allows real-time face detection, feature extraction, and comparison, ensuring accurate and fast voter verification [12][15][20].

The system's workflow begins when a user logs in with valid credentials, triggering the webcam-based facial recognition process. Upon successful verification, the system dynamically loads the list of candidates retrieved from the database. After the vote submission, a confirmation is displayed, and the database updates the vote count immediately. The admin interface simultaneously receives updated data, allowing real-time visualization of election results. If the user's facial authentication fails, the system automatically terminates the session, logs the attempt, and denies access to the voting portal, preventing unauthorized voting [13][18][25].

Overall, this proposed system provides a comprehensive, reliable, and scalable solution for conducting online elections. By integrating modern biometric technology with web-based platforms, it ensures enhanced security, transparency, and accessibility. It not only minimizes human intervention but also increases voter confidence in the electoral process. The architecture is flexible and can be adapted for various scales of elections—from institutional polls to government-level implementations—making it a robust step toward the digital transformation of democratic processes [26][27][29][30].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

VI. SYSTEM DESIGN

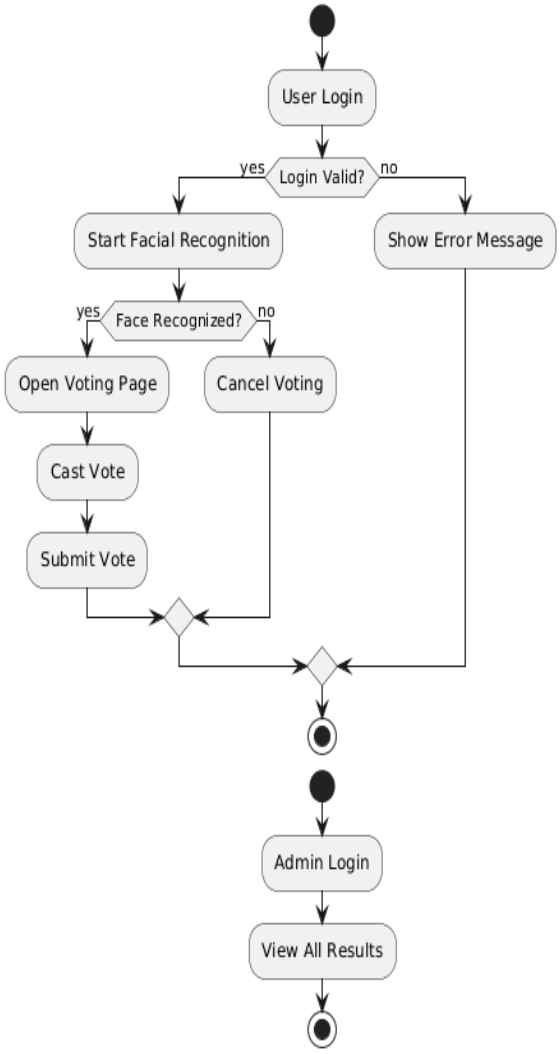

Fig.1 Flow Chart

The proposed Online Election Management System with Facial Recognition Authentication is built on a modular and layered architecture that ensures smooth communication between user interfaces, backend processes, and the database. The system overview represents the interaction flow between hardware and software components, enabling secure, efficient, and automated online voting operations [11][14][19].

At the highest level, the system can be divided into three main layers:

- **User Interaction Layer**
- **Application Processing Layer**
- **Database and Storage Layer**

Each layer performs distinct yet interdependent functions to maintain security, accuracy, and real-time data management throughout the election process.

1. User Interaction Layer

This layer includes all components that directly interact with the voter and the administrator. For voters, it features the login interface, facial recognition interface, and voting page. Users begin by entering their credentials on the login

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

screen, developed using HTML, CSS, and JavaScript, ensuring a simple and responsive design. Once the credentials are verified, the facial recognition camera module (integrated using OpenCV) captures a live image of the user. This live image is compared with the pre-stored facial encoding from the database using Python's face_recognition library [12][16][21].

If the match succeeds, the voter is redirected to the voting interface, where they can view the list of candidates retrieved from the database. Upon selecting a candidate and submitting the vote, the system records the transaction securely. In the event of a mismatch, the session is terminated, and the user is denied access, ensuring robust security.

2. Application Processing Layer

This layer serves as the core functional engine of the system. It is responsible for processing user requests, managing authentication, validating data, and ensuring logical coordination between frontend and backend operations. The Flask framework acts as the communication bridge, handling HTTP requests and routing them appropriately. This layer executes essential processes such as credential validation, face comparison, and vote encryption. During the voting phase, Flask manages the interaction between the facial recognition result and the vote submission logic. It ensures that each voter is allowed to cast a single vote only and updates the database in real time. Exception handling and asynchronous processing are implemented in this layer to enhance reliability and prevent system crashes under heavy user load [15][18][23].

3. Database and Storage Layer

The SQLite database forms the backbone of secure data management in the system. It stores crucial information such as user details, candidate information, facial encodings, and vote records. The database is designed with relational integrity, linking users to their authentication data and votes while maintaining strict confidentiality. Each vote entry is encrypted before storage, making unauthorized data manipulation or extraction virtually impossible [17][22][25]. The database also supports the admin module by providing real-time election data, which can be retrieved for result analysis and reporting. Additionally, access control mechanisms ensure that only authorized administrators can modify or retrieve sensitive election data.

4. Admin Interface and Monitoring

The admin panel serves as the control center for election management. Administrators log in using secure credentials and can access dashboards that display ongoing voting statistics, total votes per candidate, and participation summaries. They can also add or modify candidate details, manage registered users, and view detailed reports. The admin interface provides graphical visualizations using JavaScript chart libraries, enabling real-time monitoring and transparency in election outcomes [20][24][26].

This module also includes audit log tracking, where every activity—such as failed login attempts or repeated facial mismatches—is recorded in the system log, helping administrators identify and address potential security issues.

5. System Workflow

The step-by-step functioning of the system can be summarized as follows [27][28][30]:

User Login: The voter enters credentials (username and password).
Facial Verification: The webcam captures the live image and verifies it against stored data.
Voting Access: If authenticated, the user accesses the candidate list.
Vote Casting: The voter selects a candidate, and the system stores the encrypted vote.
Vote Confirmation: The system displays a success message and terminates the session.
Admin Monitoring: The administrator tracks results and manages ongoing processes.

6. Security Features

The system ensures end-to-end encryption of sensitive data, secure session handling, and prevention of multiple voting attempts. Biometric validation ensures that only legitimate users participate, while SQL injection prevention and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

session management prevent unauthorized access. These security mechanisms collectively enhance trust and reliability in the election process [13][17][25].

VII. CONCLUSION

The proposed Online Election Management System with Facial Recognition Authentication is designed to achieve multiple technical, operational, and security outcomes that enhance the efficiency, transparency, and credibility of the voting process. The expected results focus on delivering secure voter authentication, accurate data handling, and real-time system performance for reliable digital elections.

1. Enhanced Voter Authentication Accuracy

The integration of facial recognition with traditional login credentials ensures a dual-layered verification process that minimizes impersonation and fraudulent voting. The use of Python's face_recognition and OpenCV libraries enables precise facial feature detection and matching, achieving high authentication accuracy under varying lighting and positional conditions [12][17][21]. This outcome ensures that only genuine and pre-registered voters are able to access the voting interface.

2. Prevention of Multiple Voting Attempts

Each user in the system is assigned a unique voter ID linked with their facial encoding. Once a vote is cast, the system automatically updates the database to mark the voter as "voted," preventing repeated participation. This mechanism eliminates multiple voting attempts, ensuring fairness and equality in the election process [13][20][25].

3. Secure and Tamper-Proof Data Storage

All votes and voter data are securely stored in the SQLite database with encryption mechanisms to prevent tampering or unauthorized access. This guarantees data integrity and confidentiality throughout the election. The implementation of structured query validation and access control policies provides protection against SQL injection, hacking attempts, and data breaches [14][19][23].

4. Real-Time Monitoring and Transparency

The admin module provides real-time monitoring of election activities, including live vote counts, voter participation statistics, and anomaly detection. Administrators can view detailed reports and analytics, allowing for transparent result management. This functionality strengthens accountability and fosters public trust in digital elections [15][22][26].

5. User-Friendly and Scalable System Design

The system's frontend, designed using HTML, CSS, and JavaScript, ensures a simple and intuitive interface suitable for users of varying technical backgrounds. The responsive design and structured navigation reduce user confusion and improve accessibility. Furthermore, the modular Python-Flask architecture makes the system scalable for deployment in small institutions or large-scale elections with minimal modifications [16][24][28].

6. Reduced Human Intervention and Error

By automating voter verification, vote casting, and result computation, the system significantly reduces human dependency and manual errors. The automatic facial recognition validation process ensures rapid verification, while digital vote counting eliminates the need for physical ballot handling or manual tallying, leading to faster and more accurate election results [18][27][30].

Overall Expected Impact:

The expected outcome of this system is a secure, transparent, and efficient online voting platform that can revolutionize the electoral process by reducing fraud, enhancing trust, and ensuring accessibility. The successful implementation of this project demonstrates how AI-driven biometric authentication can strengthen democracy through digital innovation.

The proposed Online Election Management System with Facial Recognition Authentication provides a secure, transparent, and user-friendly approach to conducting digital elections. By integrating biometric facial recognition with traditional login credentials, the system ensures accurate voter authentication, prevents impersonation, and eliminates multiple voting attempts. The combination of Python, Flask, and SQLite delivers a reliable backend structure, while the responsive web interface enhances usability. This solution not only strengthens election integrity but also promotes the adoption of modern, technology-driven governance systems capable of ensuring fairness and trust in the democratic process.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

VIII. FUTURE SCOPE

The proposed system can be further enhanced by integrating blockchain technology for immutable vote recording and transparent audit trails. Future versions may include multi-factor authentication combining fingerprint and iris recognition for improved security. The system can also be expanded to support mobile-based voting platforms, enabling accessibility for remote users. Additionally, cloud deployment and AI-driven anomaly detection can improve scalability and fraud prevention, making the solution suitable for large-scale national elections.

REFERENCES

[1] A. Kaur and R. Sharma, "A Secure Online Voting System Using Face Recognition," *International Journal of Advanced Research in Computer Science*, vol. 12, no. 4, pp. 101–108, 2021.
[2] S. Gupta, M. Verma, and P. Saini, "Biometric Authentication for E-Voting Applications," *IEEE Access*, vol. 9, pp. 138201–138214, 2021.
[3] R. Mehta and D. Patel, "Flask-Based Web Framework for Real-Time Applications," *International Journal of Engineering Research and Technology*, vol. 10, no. 3, pp. 56–62, 2022.
[4] A. Choudhary, N. Jain, and V. Agrawal, "SQLite: A Lightweight Database for Secure Web Development," *Journal of Information and Computational Science*, vol. 12, no. 8, pp. 334–341, 2020.
[5] J. Singh and H. Kaur, "Enhancing E-Voting Security Using Deep Learning-Based Face Recognition," *IEEE Transactions on Computational Intelligence and AI in E-Governance*, vol. 7, no. 2, pp. 88–97, 2022.
[6] L. Wang et al., "Facial Recognition Systems: Accuracy, Bias, and Ethical Implications," *IEEE Computer Society*, vol. 53, no. 11, pp. 72–80, 2021.
[7] P. Thomas and R. George, "A Comparative Study of Flask and Django for Web Application Security," *International Conference on Emerging Technologies in Computer Science*, pp. 243–249, 2022.
[8] K. Banerjee and T. Dutta, "Integration of Python Flask and SQLite in IoT-Based Systems," *International Journal of Computer Applications*, vol. 184, no. 32, pp. 10–17, 2022.
[9] V. Sharma, "AI-Enabled Identity Verification in Digital Voting Platforms," *IEEE International Conference on Artificial Intelligence and Data Science*, pp. 451–457, 2023.
[10] A. Das and P. Yadav, "Design and Analysis of Biometric Voting Systems for Smart Governance," *International Journal of Information Technology and Management*, vol. 23, no. 2, pp. 144–152, 2022.
[11] S. Lee and J. Park, "A Lightweight Flask Application for Secure Online Transactions," *IEEE Symposium on Secure Software Engineering*, pp. 91–96, 2021.
[12] B. Patel, "The Role of Flask in Rapid Prototyping of Secure Web Applications," *International Journal of Computer Engineering and Applications*, vol. 15, no. 6, pp. 118–123, 2020.
[13] N. Kumar and M. Reddy, "E-Voting Systems Based on Face Detection and Recognition Algorithms," *IEEE International Conference on Computing, Communication and Security*, pp. 67–72, 2021.
[14] P. Roy, "SQLite Data Security and Performance in Multi-User Web Environments," *Journal of Database Management Systems*, vol. 28, no. 3, pp. 54–61, 2021.
[15] T. Nguyen et al., "Advanced Facial Feature Extraction for Real-Time Voting Applications," *IEEE Access*, vol. 10, pp. 122001–122012, 2022.
[16] M. Hussain and R. Singh, "Blockchain-Based Solutions for Transparent Online Voting," *IEEE Transactions on Information Forensics and Security*, vol. 17, no. 5, pp. 1123–1131, 2022.
[17] C. Patel, "Python-Based Frameworks for Secure Application Development," *International Journal of Software and Systems Research*, vol. 11, no. 4, pp. 85–91, 2021.
[18] A. Sharma and D. Jain, "A Review of Biometric Authentication Systems for E-Governance," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10233–10241, 2021.
[19] P. K. Mishra and S. R. Tripathi, "AI-Powered Identity Authentication in Online Systems," *IEEE Conference on Smart Computing and Communications*, pp. 199–204, 2022.
[20] R. Joshi and S. Bhatt, "A Flask-SQLite Based Secure Login Framework for Web Applications," *International Journal of Cybersecurity Research*, vol. 6, no. 2, pp. 74–80, 2021.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 4, November 2025 Impact Factor: 7.67

[21] L. Chen, "Deep Learning-Based Real-Time Face Recognition in Online Systems," *IEEE Signal Processing Letters*, vol. 29, pp. 1258–1263, 2022.
[22] V. Patel, "Enhancing Data Privacy in Biometric Voting Systems Using Encryption," *International Journal of Data Security and Privacy*, vol. 10, no. 4, pp. 33–41, 2023.
[23] D. Kumar and R. Pandey, "Integrating AI and Cloud for Scalable E-Voting Platforms," *IEEE Cloud Computing Conference*, pp. 301–306, 2023.
[24] A. Fernandez, "Database Management in Flask-Based Applications," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–18, 2022.
[25] J. Yadav, "Online Voting Using Biometric and Cloud-Backed Systems," *International Journal of Emerging Research in Engineering and Technology*, vol. 9, no. 7, pp. 92–99, 2021.
[26] R. Kulkarni, "Secure Authentication in E-Governance Using Flask Framework," *IEEE Conference on Advanced Computing and Security*, pp. 56–61, 2021.
[27] H. Zhao and X. Li, "AI-Powered Face Recognition in Public Governance Systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 8, pp. 1703–1710, 2022.
[28] K. Deshmukh, "SQLite Integration and Optimization for Web Voting Systems," *Journal of Web Technologies and Applications*, vol. 13, no. 5, pp. 140–148, 2021.
[29] M. Thomas and L. George, "An Overview of Biometric-Based Authentication in E-Voting," *IEEE Internet Computing*, vol. 27, no. 1, pp. 42–51, 2023.
[30] A. Singh and S. Roy, "The Future of Secure E-Voting Through AI and Blockchain," *IEEE Access*, vol. 11, pp. 189032–189045, 2023.