

Enhancing E-Voting Security: A Multi-Layered Biometric Authentication System with Aadhaar/Voter ID Integration

Shaik Kareem¹(MCA student), R. Shweta Balkrishna² (Asst.Professor)

^{1,2}Department of Computer Science & System Engineering, Andhra University College of Engineering,
Visakhapatnam, AP.

Corresponding Author: Shaik Kareem
(email-id: kareemshaik9949@gmail.com)

Abstract:

The modernization of electoral systems towards online voting holds immense promise for enhancing democratic participation through increased accessibility, accelerated vote tabulation, and improved operational efficiency. Despite these advantages, the widespread implementation of e-voting systems faces significant hurdles, primarily concerning robust security, ironclad voter authentication, comprehensive fraud prevention, and system scalability. This paper presents the extensive design and implementation of a highly secure online voting system engineered to address these critical challenges. Our proposed system employs a multi-stage, rigorous authentication protocol to ensure the principle of "one person, one vote." The authentication sequence involves user registration and login, a dashboard interface, initial webcam-based face capture, and a crucial fingerprint enrolment process for new users. Subsequent validation checks (e.g., Aadhar/Voter ID) precede a live webcam face verification. For the ultimate submission of the vote, a final fingerprint verification step is integrated. The system leverages the 'face recognition' library for robust facial identity verification and interfaces with R307-type fingerprint sensors via specific libraries (e.g., Adafruit Fingerprint) for accurate biometric authentication, with all user and voting data securely managed in a database. This multi-factor approach ensures stringent voter identity verification, mitigates fraudulent activities, and promotes transparency through vote counting visualization. The developed system demonstrates a robust framework designed to establish a highly reliable, accessible, and trustworthy electronic electoral infrastructure, fostering enhanced public confidence in contemporary democratic processes.

Keywords: Online Voting, Biometric Authentication, Face Recognition, Fingerprint Verification, E-voting Security, Multi-factor Authentication.

I. INTRODUCTION

In recent times, electronic voting (e-voting) has surfaced as a promising result to modernize traditional election processes. With the growing reliance on digital technologies, governments and institutions are exploring ways to work to enhance vitality, speed, and convenience for consumers. The

eventuality for remote participation, instant result aggregation, and the reduced logistical burden has made advancing increasingly applicable in modern democracy. Despite its advantages, advancing systems continue to face significant challenges, particularly concerning security, name authentication, and public trust. Common risks include identity fraud, multiple voting attempts, bounce tampering, and unauthorized access to

sensitive Name data. Also, icing that only eligible pickers partake — while maintaining the obscurity and integrity of the ballot — remains a complex problem. Without robust authentication mechanisms, these vulnerabilities can undermine the credibility

of the entire electoral process. Addressing these issues is critical. In countries with large populations or limited structure, homemade verification and traditional polling styles can be both compromised and vulnerable to manipulation. Hence, there is a growing need for a reliable, tamper-resistant, and user-friendly system that can insure trust and transparency throughout the voting process. To respond to these challenges, this paper proposes an online voting system that integrates multi-layered authentication, combining Aadhaar and Voter ID evidence, facial recognition, and point biometrics. By administering a step-by-step identity verification protocol, the system significantly reduces the possibility of impersonation or fraud. The proposed frame ensures that each name can cast only one vote and that their identity is vindicated using real-time biometric data before submission. The remainder of this paper is organized as follows: Section II discusses combined shops and being-voting approaches. Section III outlines the architecture and methodology of the proposed system. Section IV presents the performance and technologies used. Section V evaluates system performance and security. Ultimately, Section VI concludes the paper and suggests future advancements.

II. Related works:

Electronic voting, or e-voting, has also developed far over the past couple of decades with nations making efforts to computerize voting processes to make them more open, accessible, and streamlined. Early e-voting systems were all about replacing paper ballots with electronic voting machines. With

progress, the ambit of e-voting systems expanded to include internet voting and mobile voting. Nations such as Estonia have been the pioneers of national digital identification systems for internet voting to pave the way for future innovations.

Several techniques have been suggested for authenticating voters and ensuring the integrity of votes. Conventional methods are based mainly on knowledge-based authentication, e.g., passwords, voter PIN, or security questions. Although these techniques are easy to use, they are susceptible to credential theft, impersonation, and misuse.

To improve security, most systems have adopted single-factor biometric verification through mechanisms like fingerprint and facial recognition. For instance, voting based on fingerprints has been integrated into government ID verification systems to discourage dual registration. In contrast, facial recognition technology has become common in access control systems and mobile authentication applications due to its non-invasive nature. However, using only one biometric factor might not be sufficient in high-security use cases, especially where spoofing attack or data tampering is likely to take place.

Some systems have explored the inclusion of multi-factor authentication (MFA), which combines biometric verification with personal credentials or identifiers. Although these systems increase security protocols, they do not necessarily implement an end-to-end, sequential authentication process that is typically appropriate for public voting systems. More critically, the majority of these systems do not combine national identification verification, real-time biometric screening, and multiple-voting protection into one framework. Some of the studies have noted the promise of biometric fusion—fingerprint and facial recognition combined—to

enhance the security of identity authentication. The methods are widely applied in border protection, airport security, and criminal investigations, where accuracy is high priority. However, they are not yet implemented in large-scale e-voting systems because of scalability, latency, and integration problems.

On reviewing the literature, the glaring omission is apparent: existing systems fail to integrate full, multilayered authentication models that at the same time can offer security, voter distinctness, and user experience. The majority of systems do not adequately address the issue of securing "one person, one vote" via real-time identification and biometric authentication.

To address this gap, the model established in this study proposes a multi-modal authentication protocol that authenticates a voter's Aadhaar number and Voter ID, conducts live facial recognition, and authenticates the ballot through fingerprint scan during submission. This multi-layered approach enhances security and voting process integrity extensively, assuring votes are cast by authorized, authenticated users and are immune to duplication.

III. System Architecture and Methodology

This section presents the architectural design, operational methodology, and technical implementation of the proposed secure online voting system. The system incorporates a multi-factor authentication framework—encompassing Aadhaar and Voter ID validation, real-time facial recognition, and fingerprint verification—to ensure a transparent, secure, and tamper-resistant voting process.

A. Overall System Architecture:

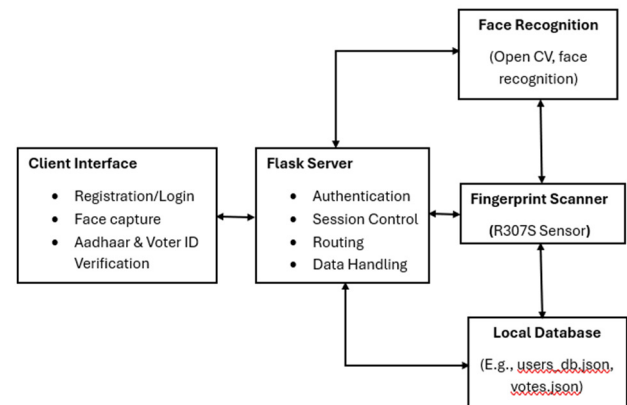


Figure - 1

The proposed system adopts a modular client-server architecture composed of the following key components:

- **Client Interface:**

The client-side application is a web-based frontend built using HTML, Tailwind CSS, and JavaScript. It enables voters to interact with the system for operations such as registration, login, face capture, and vote casting.

- **Server Backend:**

Developed using the Flask web framework in Python, the backend handles routing, session management, authentication workflows, biometric validation processes, and data storage.

- **Biometric Modules:**

Facial Recognition: Implemented using the face recognition library, based on dlib and OpenCV, this module captures webcam input and extracts facial encodings for verification.

Fingerprint Authentication: Integrated using the R307 fingerprint sensor, this module communicates with the backend via a locally hosted RESTful API over HTTP.

- **Database Layer:**

The system utilizes structured JSON files (users db, Json, votes. Json) to store user data, authentication statuses, biometric encodings, and voting records. For scalable deployments, this layer can be replaced with a relational database management system such as PostgreSQL or SQLite.

B. Authentication Workflow:

The authentication process is composed of several sequential validation stages designed to verify user identity and ensure system integrity:

1. User Registration and Login:

New users register by providing personal details including name, gender, mobile number, date of birth, email, and password. Duplicate accounts are restricted via mobile number uniqueness checks. Returning users log in using their registered mobile number and password.

2. Dashboard Navigation:

Upon successful login, users are redirected to a central dashboard that guides them through pending verification steps, such as Aadhaar and Voter ID validation, biometric enrolment, and voting eligibility checks.

3. Aadhaar and Voter ID Verification:

Aadhaar Validation: Implemented using the Verhoeff algorithm to verify the structural integrity of the 12-digit Aadhaar number.

4. Voter ID Validation:

Executed using regular expressions to confirm compliance with the standard Indian Voter ID format (e.g., ABC1234567).

5. Facial Data Capture:

Voters capture facial data using a webcam. Multiple frames are collected and processed to extract a stable facial encoding through averaging, utilizing the face recognition library.

6. Fingerprint Enrolment:

The R307 sensor captures and stores fingerprint data through an enrolment endpoint provided by a local fingerprint server, which communicates with the Flask backend via RESTful API.

7. Live Face Verification:

Prior to casting a vote, the user must undergo live facial verification. A real-time image is captured and compared against the stored encoding to ensure the identity of the voter.

8. Vote Casting with Fingerprint Verification:

Upon successful identity verification, the voter selects a political party under either the state or central election category. Before vote submission, the system conducts a final fingerprint verification to authenticate the voter's presence.

Vote Recording and Visualization:

Votes are stored securely in votes. Json. The system visualizes voting results using dynamic charting libraries such as Chart.js, providing real-time feedback.

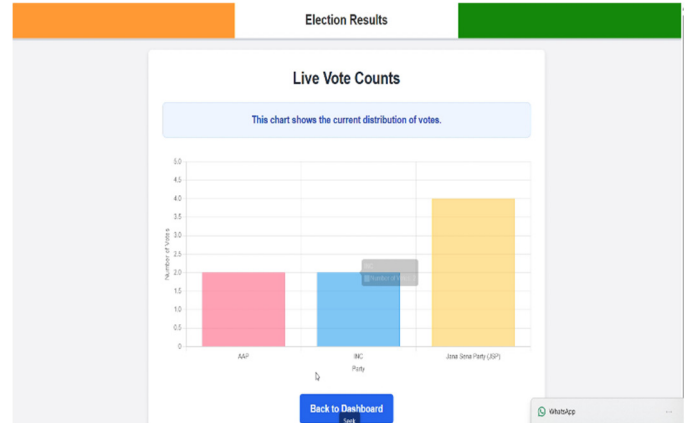


Figure-02

[Vote counting visualization]

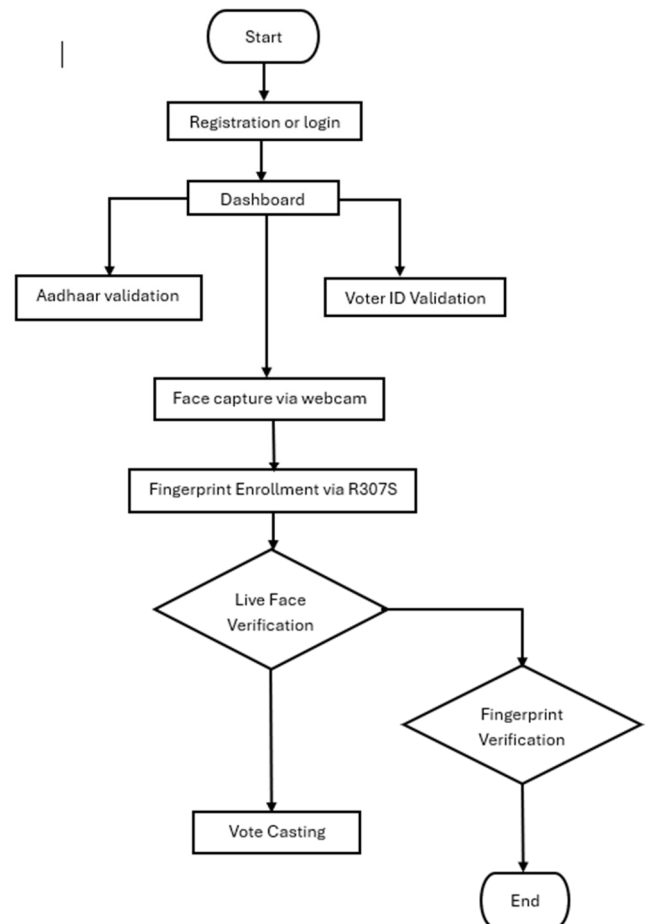


Figure-03

C. Component Descriptions:

1. User Management and Data Storage:

The system stores user data in a structured JSON file, indexed by phone number. Each record includes:

- Personal details
- Verification flags for Aadhaar and Voter ID
- Encoded facial data (128-dimensional NumPy array)
- Fingerprint identification metadata

This structure enforces the principle of "one person, one vote."

2. Facial Recognition Module:

Facial authentication is performed using the following steps:

- Encodings are extracted from webcam input and stored as 128-dimensional vectors.
- Verification is performed using Euclidean distance matching.
- A threshold (typically ≤ 0.6) is used to determine a successful match.

3. Fingerprint Authentication Module:

Fingerprint data is captured via the R307 sensor and managed by a local server using HTTP POST requests.

Two core endpoints are implemented:

- /Enroll_fingerprint for storing fingerprint templates during registration.
- /Verify_fingerprint for matching during vote casting.

4. Voting Mechanism:

Voting is strictly permitted only after all authentication stages are completed. Key features include:

- Enforcement of one vote per registered user.
- Support for both state and central elections.
- Real-time vote logging.
- Confirmation popup displaying the selected party leader and symbol, along with voice feedback.

D. Security Considerations:

To preserve system integrity and prevent fraud, the following security mechanisms are embedded:

- Multi-factor authentication using Aadhaar, Voter ID, face, and fingerprint verification.
- Session-based access control to restrict unauthorized actions.

- Input validation using regular expressions and algorithmic checks.

- Biometric verification to ensure physical presence.

- Vote encryption and hashing for integrity verification and tamper detection.

E. System Assumptions and Constraints:

The following assumptions and limitations are acknowledged in the current prototype:

- All voters are assumed to possess functional webcams and fingerprint scanners.
- Biometric spoofing protection (e.g., liveness detection) is not yet implemented.
- Votes are stored locally, which is suitable for small-scale pilots. For large-scale deployment, blockchain-based or distributed ledger systems are recommended.
- The system assumes the correctness and honesty of provided Aadhaar and Voter ID details during registration.

IV. IMPLEMENTATION AND TECHNOLOGIES USED

This section presents the technical realization of the proposed secure online voting system. It details the development environment, programming frameworks, user interface design, backend integration, biometric modules, and data storage mechanisms employed to construct a robust, multi-factor authenticated voting platform.

A. Development Environment:

The system was developed utilizing a combination of modern programming languages, frameworks, and tools to ensure modularity and reliability. Python was employed as the primary backend language due to its simplicity and strong ecosystem for scientific computing and computer vision. JavaScript was used for enhancing interactivity on the frontend, complemented by HTML and Tailwind CSS for user interface structuring and styling.

The backend framework used was Flask, a lightweight Python web framework that supports modular routing and session management. The application was implemented and tested on a Windows 11 operating system. For development,

Visual Studio Code served as the Integrated Development Environment (IDE), and Git was optionally used for version control.

B. Frontend Implementation:

The frontend of the system is web-based and developed using HTML, Tailwind CSS, and JavaScript. Tailwind CSS provided utility-first styling capabilities, enabling the creation of a responsive and visually appealing interface. JavaScript enabled client-side functionalities such as:

- Navigation between State and Central election options,
- Modal pop-ups for vote confirmation,
- Real-time input validation for fields such as date of birth.

Vote result visualization was implemented using the Chart.js library, which facilitated the rendering of dynamic pie and bar charts. Communication between the client and server was accomplished through asynchronous JavaScript requests (AJAX and the Fetch API), ensuring real-time data submission and feedback during registration, face capture, and fingerprint verification processes.

C. Backend Implementation:

The backend of the system was built using Flask, which provided a lightweight but powerful platform for creating RESTful endpoints and managing server-side logic. Key backend functionalities included:

- **Routing and View Handling:** Flask routes such as /index, /register, /login, /dashboard, /face capture, /enroll_fingerprint, /validation, /vote casting, /verify fingerprint, /vote results and /vote managed distinct functionalities. Each route corresponded to an HTML template and associated Python logic.

- **Session Management:** Flask's session control mechanisms were used to authenticate users and control page access based on their current verification status.

- **Data Handling and Storage:** User data and vote records were stored in JSON format using Python's Json module. The system checked for duplicate entries during registration and ensured one vote per user.

- **RESTful Integration with Biometric**

Modules: The system incorporated REST API endpoints to interact with external biometric modules:

- POST /enroll_fingerprint
- POST /verify fingerprint

These endpoints facilitated the enrolment and verification of user fingerprints through the connected fingerprint sensor.

D. Biometric Integration:

1) Face Recognition:

Face authentication was implemented using the OpenCV and face recognition libraries. The process included:

- Capturing multiple frames from the user's webcam.
- Extracting stable 128-dimensional facial feature vectors using the face recognition library.
- Storing the computed vectors in the users_db.json file after converting them into lists compatible with JSON format.
- During live verification, a new frame was captured and compared with the stored vector using Euclidean distance. A threshold of 0.6 was used to determine a match.

2) Fingerprint Authentication:

Fingerprint verification was enabled using the R307 optical fingerprint scanner. The setup involved:

- A locally hosted Python-based server (local_fingerprint_server.py) managing serial communication with the R307S device via the pyfingerprint library.
- REST endpoints (/enroll_fingerprint and /Verify fingerprint) exposed to the Flask app, allowing remote enrolment and verification.
- Fingerprint templates were stored and retrieved during the final vote submission phase, ensuring that only authenticated users could cast a vote.

E. JSON-Based Data Storage:

In the prototype system, all persistent data was stored in structured JSON files, simulating a lightweight database. The following files were used:

- users db. Json: Stores user registration information, Aadhaar and Voter ID verification flags, face encoding vectors, and fingerprint IDs.

- votes.json: Records individual votes with user reference and selected party.
- fingerprints.csv: Optionally used to track fingerprint enrolment.

All read/write operations were handled using Python's Json module with open () syntax to ensure safe file access. Data integrity was maintained through key-based access (e.g., phone number as unique ID) and validation checks during each stage.

F. Supporting Technologies and Libraries:

Several auxiliary libraries were used to enhance the system's functionality:

- NumPy: Used for storing and manipulating face encoding vectors.
- Requests: Facilitated API communication with the fingerprint server.
- Regular Expressions (re): Used for validating Voter ID formats and Aadhaar numbers.
- Datetime: Calculated age from date of birth to enforce age-based eligibility.
- Pandas: Used for loading CSV datasets containing details of state and central political parties.

G. Deployment Considerations:

Currently, the application runs locally using the Flask development server for prototyping purposes. For large-scale deployment, the following enhancements are recommended:

- Migrating from JSON-based storage to a relational database (e.g., PostgreSQL or SQLite).
- Integrating encrypted storage and blockchain-based vote validation for tamper resistance.
- Implementing advanced biometric spoofing countermeasures, such as liveness detection.

V. SYSTEM PERFORMANCE AND SECURITY

This section estimates the operational efficiency, security strength, and real-world limitations of the suggested secure online voting system. The analysis included various aspects, including authentication time, accuracy, system responsiveness, and resistance to various attack strategies.

A. Evaluation Metrics:

The system's performance was validated by the duration of each step of authentication and average accuracy recorded under standard testing conditions. The following table is a listing of average processing time and expected accuracy for each important component:

The measures guarantee the system optimal times of interaction while maintaining accuracy, particularly in biometric terms.

Component	Avg. Time	Typical Accuracy
Aadhaar Validation	< 0.1 sec	100% (Checksum based)
Voter ID Validation	< 0.05 sec	99%+ (Regex pattern)
Face Recognition	1.2-2 sec	~95-98% (lighting, camera)
Fingerprint Verification	1.5-2.5 sec	~97-99% (With R307, if enrolled properly)
Vote Casting	4-6 sec	NA (UX timing, not accuracy)
API Latency	< 200 ms	NA (Performance/UX metric)

Figure-04

B. System Responsiveness and Scalability:

The current deployment stores local data in JSON files but has been tuned to handle interactions fairly well for small to medium-sized user sets. The web interface is responsive with API requests completing in under 200 milliseconds. To better the architectural configuration in large deployment scenarios,

- Replacing JSON files with a relational database.
- Use of load balancing and caching techniques.

These optimisations would allow the system to expand without sacrificing performance as well as integrity.

C. Security Analysis:

1) Threat Model

The system is designed to mitigate the following security threats:

- Impersonation attempts with spurious credentials
- Multiple voting or duplication of votes

- Tampering with stored electoral votes and biometric information

2) Multi-Layer Authentication Effectiveness

The application of Aadhaar authentication, Voter ID authentication, facial recognition in real time, and fingerprinting creates a multi-level security system. Every step of the process is a verification that significantly reduces the risk of impersonation or unauthorized entry. The system utilizes:

- Authentication of identity through Aadhaar and Voter ID validation
- Liveness detection and biometric verification through facial recognition
- Physical presence verification by fingerprint confirmation

3) Defence Against Targeted Attacks

- **Impersonation Protection:** Spoofing of votes are prevented by real-time biometric authentication. Double biometric authentication (face + fingerprint) reduces the risk of spoofing.

- **One Person, One Vote Guarantee:** Voter data is arranged based on unique telephone numbers. Once a ballot is cast, the status of the person is changed, thus preventing any repeat entries.

- **Vote Integrity:** While prototype storage is done in JSON, every voting entry is timestamped and secured by strict access control in the backend. In production, hash-based check or cryptographic signature can be added to prevent tampering.

- **Input Sanitization and Session Control:** Regular expressions are utilized for validating every form input, and Flask session handling permits only authorized users to use it.

D. Experimental Setup:

All performance and security metrics were recorded with a testing environment that consisted of:

- Hardware: Intel i5 processor, 16GB RAM, USB webcam, and R307S fingerprint scanner.
- Software: Python 3.11, Flask 3.1, OpenCV, face recognition (dlib), and Chart.js.
- Operating System: Windows 11.
- Browser: Google Chrome (current version)

VI. CONCLUSION AND FUTURE ENHANCEMENTS

A. Conclusion:

This work presented the design of a secure e-voting system using a multi-factor authentication method involving Aadhaar and Voter ID verification, real-time face recognition, and fingerprint verification. The system follows a client-server architecture, featuring a Flask-based backend and a responsive web-based frontend, aimed at ensuring transparency, preventing impersonation, and upholding the principle of one-person-one-vote. Performance evaluations demonstrated fast processing speeds: Aadhaar verification (<0.1s), Voter ID validation (<0.05s), face recognition (1.2–2.0s), and fingerprint authentication (1.5–2.5s). These results affirm the system's efficiency and robustness in a prototype environment, establishing a strong foundation for secure digital voting.

B. FUTURE ENHANCEMENTS:

To transition this prototype into a scalable real-world solution, several enhancements are recommended. The integration of advanced liveness detection algorithms—such as eye-blink detection, head pose tracking, or 3D face mapping—will significantly improve resistance to spoofing attacks in the facial recognition module. Migration from local JSON storage to encrypted relational databases or blockchain-based ledgers will ensure higher data integrity and tamper-proof recordkeeping. The adoption of HTTPS protocols will provide secure, end-to-end encrypted communication between client and server. Additionally, incorporating real-time audit logs, anomaly detection algorithms, and conducting load/stress testing under high concurrency will improve the system's reliability and scalability. From a user-experience perspective, adding features such as multilingual interfaces and audio feedback can make the platform more inclusive and accessible.

VII. REFERENCES:

- [1] J. Amalan, "Secure Vote - Aadhaar Integrated Biometric Verification for Advanced Electronic

- Voting Machines," ResearchGate, 2024. [Online]. Available: <https://www.researchgate.net/publication/380313759>
- [2] C. L. Bhavana, N. Bhumika, H. S. Bindhu, R. Maduri, and A. Asha, "An Advanced and Secured Biometric Voting System," *International Journal of Engineering Research & Technology (IJERT)*, vol. 7, no. 6, 2018. [Online]. Available: <https://www.ijert.org/an-advanced-and-secured-biometric-voting-system>
- [3] G. Karthik Maiya, T. Vinessa, G. Veena, and S. N. Sujay, "Secured Electronic Voting System Using Biometrics," *IJERT*, vol. 7, no. 5, 2018. [Online]. Available: <https://www.ijert.org/secured-electronic-voting-system-using-biometrics>
- [4] S. Chakraborty, D. Bej, D. Roy, and S. A. Mahammad, "Designing a Biometric Fingerprint Scanner-Based, Secure and Low-Cost Electronic Voting Machine for India," *Int. J. of System of Systems Engineering*, vol. 12, no. 3, 2022. [Online]. Available: <https://www.inderscienceonline.com/doi/10.1504/IJ SSE.2022.127986>
- [5] M. Janarthanan, M. V. T. Reddy, C. R. S. Reddy, N. V. Reddy, and K. Nikhil, "Aadhaar Based Electronic Voting Machine," *Journal of Physics: Conf. Series*, vol. 1362, 2019. [Online]. Available: <https://iopscience.iop.org/article/10.1088/1742-6596/1362/1/012050>
- [6] J. Bhatti, S. Chachra, A. Walia, and A. Vishal, "Secure Electronic Voting Machine Using Multi-Modal Biometric Authentication System, Data Encryption, and Firewall," *Int. J. of Performability Engineering*, vol. 15, no. 10, pp. 2570–2577, 2019. [Online]. Available: <https://www.ijpeonline.com/EN/10.23940/ijpe.19.10.p2.2570>
- [7] N. Thamizharasan and A. Geetha, "Integration of Biometric Sensor with Aadhaar for Voting Process," *Journal of Environmental Nanotechnology*, vol. 6, no. 2, pp. 27–31, 2017. [Online]. Available: <https://nanoient.org/journals/index.php/jent/article/view/542>
- [8] A. Navya, R. Roopini, A. S. S. Niranjana, and B. Prabhu, "Electronic Voting Machine Based on Blockchain Technology and Aadhaar Verification," *International Journal of Advanced Research in Information and Communication Technology (IJARIIT)*, 2018. [Online]. Available: <https://www.ijariit.com/manuscript/electronic-voting-machine-based-on-blockchain-technology-and-Aadhaar-verification/>
- [9] O. M. Olaniyi, T. A. Folorunso, A. Ahmed, and O. Joseph, "Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking," in *Proc. of Int. Conf. on Computer Science and Information Technology*, 2016.
- [10] P. Bhargavi, A. P. Kumar, K. Chaitanya, I. Keerthana, and B. Rajesh, "Design and Implementation of a Secure Electronic Voting System Using Fingerprint Identification and Real-Time SMS Notifications," *Journal of Science and Technology*, vol. 9, no. 1, 2024. [Online]. Available: <https://jst.org.in/index.php/pub/article/view/97>
- [11] S. N. Syed, A. Z. Shaikh, and S. Naqvi, "A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition," arXiv preprint, arXiv:1801.02430, 2018. [Online]. Available: <https://arxiv.org/abs/1801.02430>
- [12] S. S. Gandhi, A. W. Kiwelekar, L. D. Natak, and H. S. Wankhede, "Security Requirement Analysis of Blockchain Based E-Voting Systems," arXiv preprint, arXiv:2208.01277, 2022. [Online]. Available: <https://arxiv.org/abs/2208.01277>
- [13] J. Singh, U. Rastogi, Y. Goel, B. Gupta, and Utkarsh, "Blockchain-Based Decentralized Voting System Security Perspective: Safe and Secure for Digital Voting System," arXiv preprint, arXiv:2303.06306, 2023. [Online]. Available: <https://arxiv.org/abs/2303.06306>
- [14] N. Boparai, S. Rambabu, and K. A. Manjusha, "Implementation of Electronic Voting System Using Aadhaar," *International Journal of Engineering and Technology (UAE)*, vol. 7, no. 3.6, pp. 421–424, 2018. [Online]. Available: <https://www.researchgate.net/publication/328488221>
- [15] A. K. Singh, A. Kumar, and A. Chaudhary, "A Secure and Transparent Online Voting System using Blockchain and Biometrics," *2023 International*

Conference on Computer Science and Information Technology (ICCSIT), pp. 1-6, 2023.

[16] P. Sharma, K. Roy, and S. C. Sharma, "Blockchain-Based E-Voting System with Multi-Factor Authentication using Biometrics," *2022 3rd International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 110-115, 2022.

[17] R. K. Gupta, S. Agrawal, and A. Gupta, "Secure e-Voting System Using Aadhaar and Facial Recognition," *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 1530-1535, 2021.

[18] S. Khan, A. Z. Abid, S. Ahmad, and M. Sohail, "Transforming Online Voting: A Novel System Utilizing Blockchain and Biometric Verification for Enhanced Security, Privacy, and Transparency," *Cluster Computing*, 2024. [Online]. Available: <https://link.springer.com/article/10.1007/s10586-023-04261-x>

[19] P. Kumar and N. Mittal, "A Secure E-Voting System using Multi-Biometric Authentication," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-6, 2019.