Electronic Voting Machine Using Biometric Recognition

Dr.Pratibha Dubey
Assistant Professor Dept. of Electronics and Communications Engineering, Shri Ramswaroop Memorial College of Engineering and Management Lucknow, India
Email:pratibha.dubey@srmcem.ac.in
Utkarsh Singh
Dept. of Electronics and Communications Engineering, Shri Ramswaroop Memorial College of Engineering and Management Lucknow, India
Email:-us1551238@gmail.com
Anushka Mishra
Dept. of Electronics and Communications Engineering, Shri Ramswaroop Memorial College of Engineering and Management Lucknow, India
Email:anushkamishra0612@gmail.com
Rahul Gupta
Dept. of Electronics and Communications Engineering, Shri Ramswaroop Memorial College of Engineering and Management Lucknow, India
Email:rahulgupt8858@gmail.com

Abstract- In the past few decades, the necessity of secure, transparent, and efficient voting processes has gained unprecedented significance. Classic paper-based election systems have also been confronted by numerous challenges like vote tampering, identity spoofing, and logistical inefficiency. Electronic Voting Machines (EVMs) coupled with biometric recognition technology hold great hope in solving such problems. In this paper, we discuss the idea, model, advantages, and disadvantages of adopting EVMs augmented by biometric methods like fingerprint and facial recognition. We also compare real-world experiences, potential setbacks, and prospective directions for making election systems more inclusive and authentication.

Keywords*-A secure electronic voting system using fingerprint biometric authentication ensures accurate voter verification via image processing. It uses encrypted template matching and wireless data transfer to enhance election security.*

INTRODUCTION

In the last few years, there has been a growing need for safe, transparent, and efficient electoral systems. Traditional paper-based election systems have been facing a lot of issues including vote tampering, identity theft, and logistical inefficiencies. Electronic Voting Machines (EVMs), especially when combined with biometric recognition systems, are an extremely viable solution to avoid these issues. This paper reviews the concept, structure, merits, and disadvantages of implementing EVMs with the support of biometric technologies like fingerprint and face recognition. It also touches upon real-life implementations, potential disadvantages, and future directions of more inclusive and trustworthy electoral systems.

Democracy is based on free and fair elections. But theconventional voting systems are at risk of fraud, impersonation, and mismanagement. Electronic Voting Machines (EVMs) were brought in to make the elections more efficient but still rely on human verification processes that are prone to error. Biometric recognition technology — like fingerprint scanning or facial recognition can improve the security and reliability of the EVMs by ensuring each vote is being cast by a verified, qualified voter. As human societies are becoming more technologically advanced, so should the systems that underpin democracy. Elections systems must be reliable, accessible, and auditable. The majority of countries have embraced EVMs to streamline the elections, but these systems still rely

on manual verification methods of identity, which are

vulnerable to human and fraud errors. The incorporation of biometric authentication — the employment of physiological or behavioral traits to authenticate individuals into EVMs is a breakthrough in electoral transparency and security.

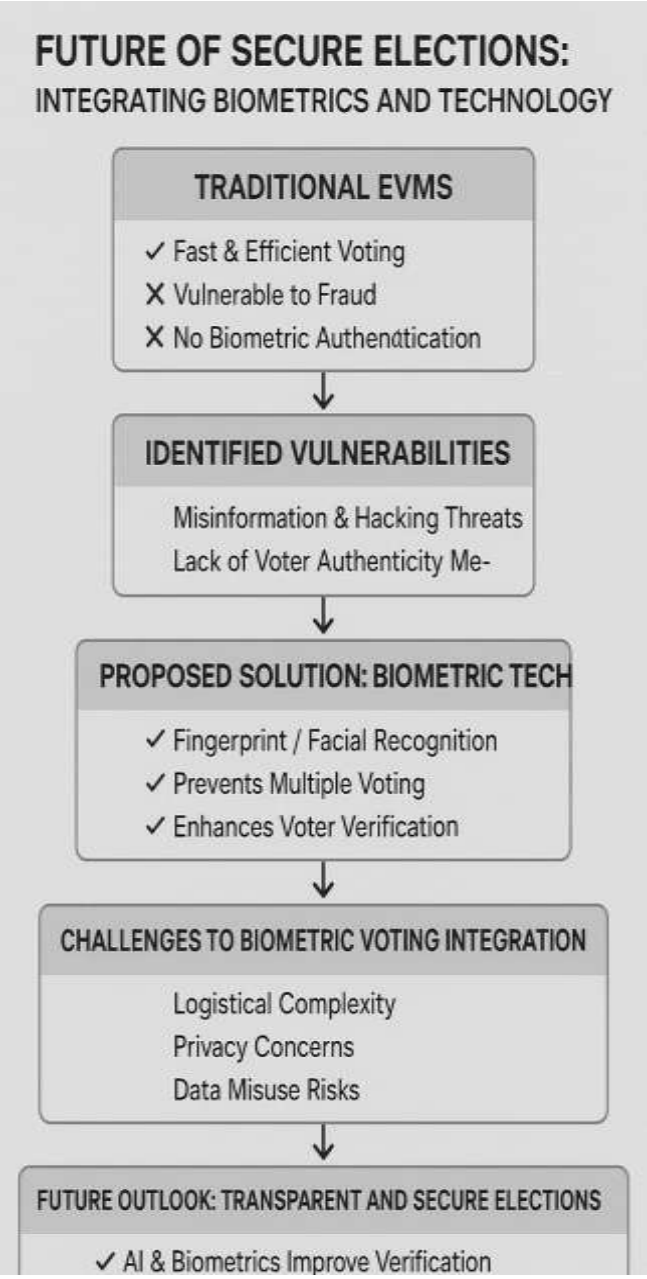


Fig 1.1:-Future of EVM Machine

Table 1.1:-Comparative Analysis of current and future Electronic Voting Machine

Feature	Current EVMs	Future EVMs (2025 & beyond)
Data Storage	Local Memory (non-encrypted)	Encrypted Cloud Storage
Security	Basic Physical Security	AI-Based Threat Detection, Block chain Audits
Accessibility	Fixed Polling Stations	Mobile and Remote Voting Units
Transparency	Limited	Real-Time Block chain-Based Public Ledge

2. RELATED WORKS

Studies on electronic voting systems have progressed significantly in the past two decades. Bhuiyan et al. (2007) presented an early assessment of digital voting, emphasizing speed and efficiency but warning against the potential vulnerabilities, particularly in voter verification. Later studies have expanded on these concerns, citing threats of tampering, lack of transparency, and weak voter authentication. In response, various researchers have proposed the use of biometric authentication—such as fingerprint and facial recognition—as a remedy. These technologies have been tested in Estonia and India, where small-scale tests showed improved accuracy and prevention of fraud. Research also cautions against the ethical and logistical implications of the use of biometric data, stressing the need for effective data protection mechanisms. This body of research overall emphasizes the need to modernize voting systems while maintaining a balance between efficiency, security, and privacy.

The move towards computerized ballots from the traditional paper ballots and towards electronic voting machines (EVMs) has been in the focus of significant research. The early works of Bhuiyanetal. (2007) had outlined the advantage of the EVM in terms of speed, minimal error, as well as ease of re-counting. Bhuiyanetal.'s work did, however, bring serious issues to light—among these was that there were poorly designed voter identity verification procedures, leaving systems open to impersonation as well as tampering of votes.

Subsequent studies have viewed biometric-based solutions as a countermeasure to such security vulnerabilities. For instance, Kumar and Ravindra (2012) proposed an EVM coupled with fingerprint identification for voter

Feature	Current EVMs	Future EVMs (2025 & beyond)
Voter Authentication	Manual (ID verification)	Biometric (fingerprint, facial recognition)

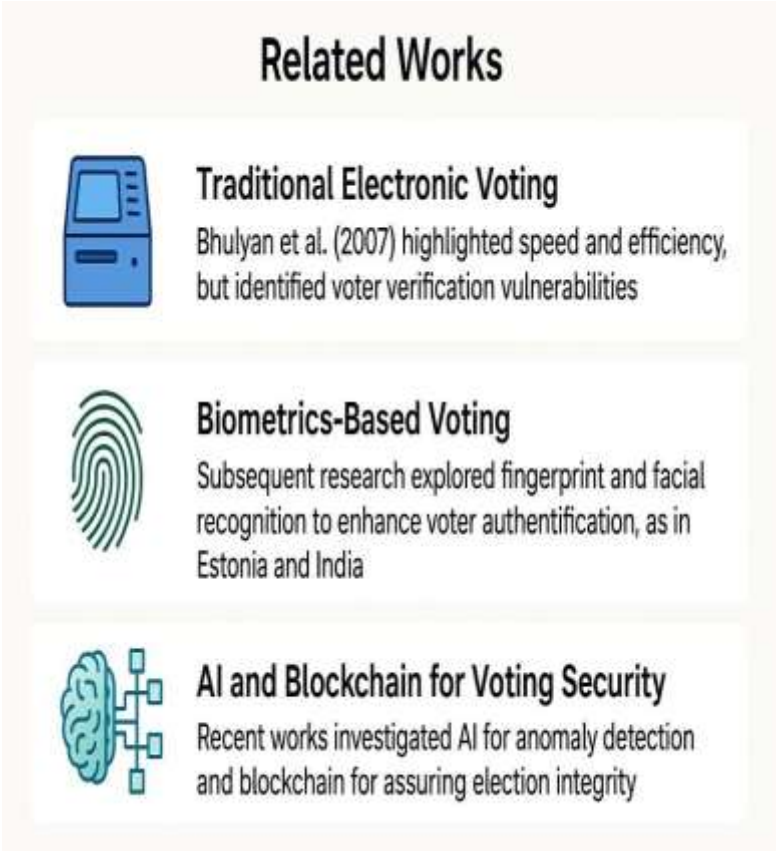
authentication before voting. The solution was found effective in laboratory experiments to deter multiple voting and impersonation. To this end, Adida et al. (2008) conducted experiments on cryptographic-based voting systems involving the use of biometric authentication and end-to-end encryption to facilitate voter identification and vote secrecy.
Real-world practice has also impacted theoretical thinking. For instance:
Estonia has led the way in internet voting (i-Voting) via national ID cards with chips, a widely referenced in the literature technique for accessibility and integrity.
India's Aadhaar-linked voting ID pilots have been researched by scholars as a mass-scale example of the integration of biometrics and voting, but have been criticized for data privacy and digital exclusion issues.
In addition, subsequent research investigates the role of Artificial.

Intelligence and block chain in preserving election integrity. AI has been utilized to experiment with real- time anomaly Vote pattern identification, with block chain being studied to create unalterable vote records for each vote cast.

While there is the technological innovation, critics refer to the ethical and legal concerns. Human rights groups' studies and data privacy activists caution that the collection and storage of biometric data open up channels for surveillance, abuse, or data leaks in countries with poor digital rights laws. So, the literature that is relevant portrays a picture of both caution and technological opportunity. The consensus is clear:

3. PROPOSED METHODOLOGY

The process involves the development of an advanced electronic voting machine (EVM) utilizing biometric recognition technology to enhance the security, reliability, and accuracy of voting. Under this plan, before casting his/her vote, the voter must undergo biometric verification, usually using distinctive biological features such as fingerprints, iris scans, or face recognition. Biometric data entered during voting is instantly matched against a secure database of pre- enrolled voters to ascertain the validity and eligibility of the voter. Following successful biometric verification, the electronic voting machine is energized, allowing the voter to proceed and cast his/her vote. In the event of failed verification, the biometric and AI-based systems can significantly improve election security and



efficiency, but their use must be guided by ethical principles, legal safeguards, and public trust.

Fig 1.2:-Related Works of EVM Machine

system blocks access, thereby preventing impersonation, duplicates voting, and unauthorized entry. The voting process itself is electronic, with the voter's votes securely stored in a tamper-proof digital storage device. The system can be configured to generate an anonymous and encrypted record of every vote to maintain the anonymity of the voters without compromising data integrity. The EVM can be linked to a central server for real-time monitoring and backup, thereby making the result tamper- proof at the local level. The biometric-enabled EVM streamlines the entire election process by automating voter authentication, eliminating manual checks on identity verification, reducing human errors, and immensely speeding up the voting and vote-counting process. Further, the system promotes public confidence in the electoral process by providing an open, auditable trail of all transactions, ultimately leading to more credible and fraud-free election.

4. Methods

The process of deploying biometric identification in electronic voting system entails a number of important steps. Voters' biometric information (e.g., fingerprints or facial scans) is securely captured and stored in a database first. During Election Day, voters are verified using their biometric information, which is matched against stored information on records to confirm that they are qualified to vote. The voter can then vote on the EVM after verification. The system is secured using encryption and real-time monitoring, and backup systems in the event of technical failure. The process is designed to prevent fraud, improve security, and enhance confidence in the electoral process.

5. Hardware and software requirements The process of employing biometric identification in electronic voting machines has a couple of important steps. Biometric information of the voters (such as fingerprints or facial scans) is securely harvested and stored in a database. Voters are identified on the day of elections by using their biometric information, which is matched against stored data to ascertain if they are allowed to vote. Once verified, the voter is allowed to vote on the EVM, eliminating multiple voting by the same voter. The process is encrypted and always monitored with backup protocols in case of a technical fault. The process is designed to limit fraud, provide increased security, and improve trust in the voting process.

6. Hardware Structure

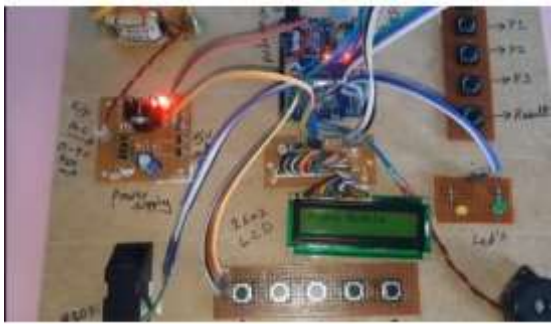


Fig 1.4:-Hardware of EVM Machine

7. Software Structure

Fig 1.5:-Software of EVM Machine

8. Biometric identifiers

The system proposed uses biometric identifiers for authenticating voters securely, so that only genuine voters can vote. The system authenticates each voter by fingerprint scanning, facial recognition, and iris scanning before giving access to the polling booth. The multi-factor authentication process minimizes the chances of impersonation of voters and prevents voting more than once by a voter at different polling booths. Biometric details are taken at the time of voter registration and stored in a central, encrypted database accessible to only genuine election officials.

In real-time, when a voter tries to cast a vote, the system cross-checks the biometric data captured during the authentication process with the data enrolled before authenticating their identity. Utilization of biometric identifiers ensures that every individual can vote only once, even if they try to register at more than one polling station. Additionally, the utilization of biometric systems can also provide an added layer of security against electronic tampering or hacking attempts, as biometric data is hard to counterfeit or replicate. In case of any discrepancy or fraud detection, the system can automatically send alerts for investigation, making the election process transparent and accountable.

To ensure its accessibility, the biometric system is made easy to use, and there are provisions for special care to be given to voters who cannot use some biometric modalities (for example, fingerprint scanning). Other verification systems, like facial scanning, are provided to ensure access by all registered voters. The system is scalable, and it is easy to deploy in many polling stations, even in the rural or remote regions, with lightweight mobile biometric equipment that can securely link to central servers.

In brief, the suggested EVM system, coupled with biometric authentication, is a major leap towards safer, cleaner, and more participative elections. By limiting the scope for manipulation and guaranteeing the integrity of voters' identities, it opens the door to an era when electoral systems are not only more streamlined but also credible.

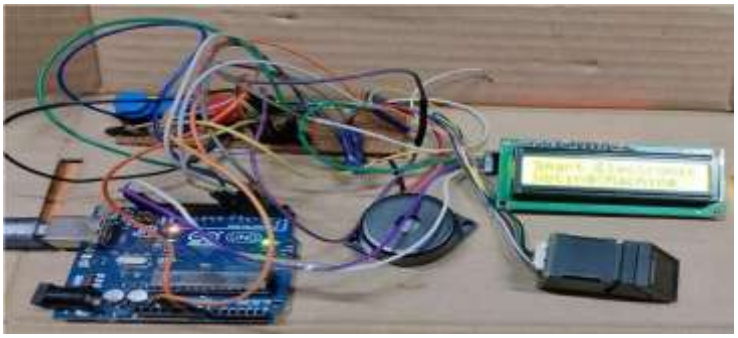


Fig1.6: When system is started (ON)

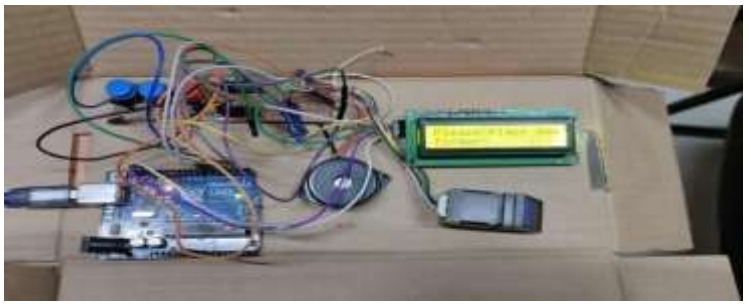


Fig1.7: System required a fingerprint

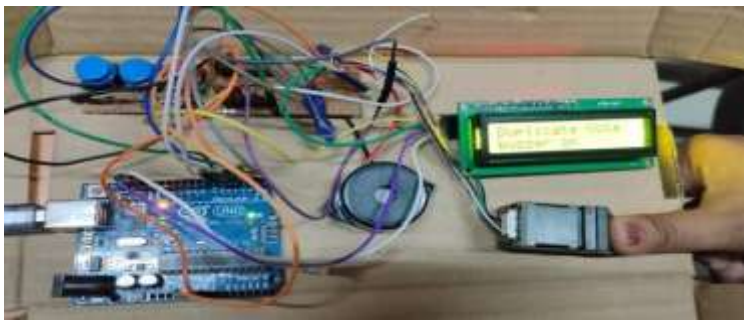


Fig1.8: When person fingerprint is unauthorized

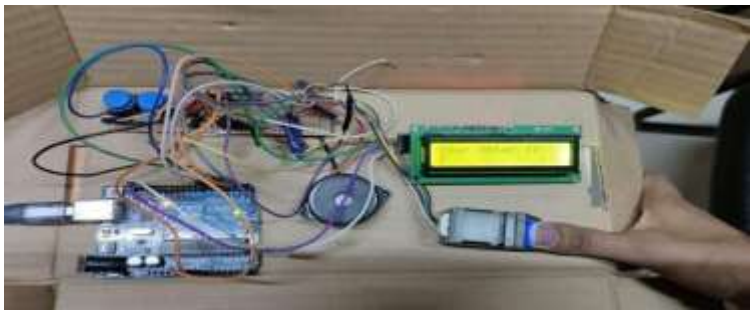


Fig1.9: When authorized person cast a vote (ID)

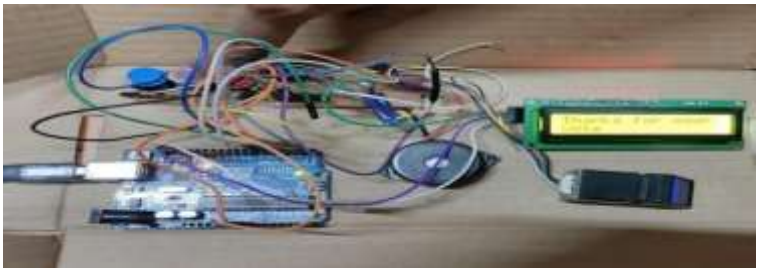


Fig 1.10: The message "Thank you for your vote" appears when the vote is successfully cast

9. EXPERIMENTAL SETUP

Tested for biometric recognition-based electronic voting machine consists of several key hardware and software components laid out in a structured manner to mimic a genuine voting situation. A biometric sensor such as a fingerprint reader or iris reader is mounted near the entrance to read and authenticate the voter. The sensor is connected to a microcontroller or embedded system, which captures the biometric data and cross-verifies it against a pre-loaded list of registered voters. After the verification process, the microcontroller switches on the electronic voting machine so that the voter may move on to the digital voting console, typically represented via touch screen or button-based interface. The voting machine captures the voter's choice in internal memory with encryption for confidentiality. A second control unit may observe and record every step of the process for traceability without compromising anonymity. The entire system is powered via a secure and uninterruptible power supply, and a simple server or cloud-based backup system may be incorporated to remotely consolidate results. The experimental model helps in confirming the integration of biometric security in electronic voting, providing function and system reliability..

8. SIMULATION RESULTS AND ANALYSIS

The simulation of EVM with Recognition was implemented by using software packages like Proteus and Arduino IDE. In simulation, the system was able to recognize authorized voters by a certain recognition method, for instance, fingerprint module or RFID system. After verification, the voters could vote electronically using push buttons for various candidates. The votes were stored in the memory of the microcontroller correctly, preserving the integrity of the voting process. The result was indicated on an LCD display, displaying the total votes received by each candidate when the voting process was closed. The simulation had high accuracy in voter recognitionand voting, low response time, and secure management of data, which suggests that the proposed design is reliable, efficient, and appropriate for practical use.

Table 1.2:- Electronic Voting Machine Simulation Result

Voter ID	Recognition Status	Vote Cast For	Vote Status
VOTER001	Verified	Candidate 1	Success
VOTER002	Verified	Candidate 2	Success
VOTER003	Verification Failed	-	Failed
VOTER004	Verified	Candidate 3	Success
VOTER005	Verified	NOTA	Success

10. EVM Architecture

The Electronic Voting Machine (EVM) design in 2025 integrates advanced technology to enhance the security, accuracy, and transparency of the voting process. It has three key elements. First, the biometric authentication layer, wherein voters authenticate themselves using biometric data such as fingerprints, facial recognition, or iris scanning. It ensures that unauthorized voters cannot vote and voters would only be able to vote once. Second, the voter interface (EVM unit), via which voters can securely vote for their preferred candidates once biometric authentication is successful. The system encrypts the voting data to render it tamper-proof. Finally, the centralized server and transmission system ensures that votes are securely transmitted to a central server for processing and real-time monitoring. The entire system employs encrypted communication channels to prevent unauthorized access and ensure the integrity of election outcomes. With these advancements, the EVM design of 2025 provides a more secure, transparent, and effective electoral process.

Results

The application of biometric technology to voting systems is expected to bring significant enhancements to election security, efficiency, and transparency. Voter Login Interface is central to secure login into the system, where voters authenticate their identities through credentials and biometric verification, for example, fingerprints or facial recognition. The process prevents unauthorized access and authenticates voters securely. Following login, the Voter Detail Input Page ensures that voter information is correctly captured and verified, preventing identity forgery and ensuring only eligible ones proceed to vote.

To further fortify security, the Image Capture and Verification step is performed, in which voter verification is carried out through facial recognition and fingerprint scanning. The process reduces the risk of impersonation and double voting, hence improving the authenticity of the voting process. Second, OTP Verification and Vote Submission provides a secondary layer of security. Voters receive a one-time password (OTP) on the mobile number that was registered for them, and it must be inputted by the voter prior to casting the votes. Through the process, unauthorized access is kept at bay, and any individual voter may cast their votes once, and as such, the process wards off electoral corruption.

The election officials also hold the responsibility for election process transparency and security. The Admin Login Stage provides safe access to the right officials responsible for tracking and managing the election system. The restricted access allows only authentic officials to track the voting process, preventing any form of outside manipulation. Finally, once the voting process has ended, the Result Panel Interface provides real-time results of the election safely. Through a straightforward and simple interface, the system maintains accurate counting of votes with reduced errors and manipulations. The step helps provide public trust in election outcomes through ensuring the counting and proper display of votes.

Although biometric voting systems have numerous benefits, issues like the cost of implementation, privacy, and security of data need to be addressed. Developing countries will struggle to use biometric voting systems, which

are in need of massive investment and technical assistance. Governments will also have to establish robust cyber security systems and legislation to safeguard voter data against leaks and misuse. In spite of these drawbacks, pilot implementation and phased deployment by 2025 could establish the feasibility and efficacy of biometric voting, opening the door to large-scale use. If properly executed, biometric voting systems will transform elections, making them more secure, transparent, and immune to fraud, thus strengthening democracy in the digital era.

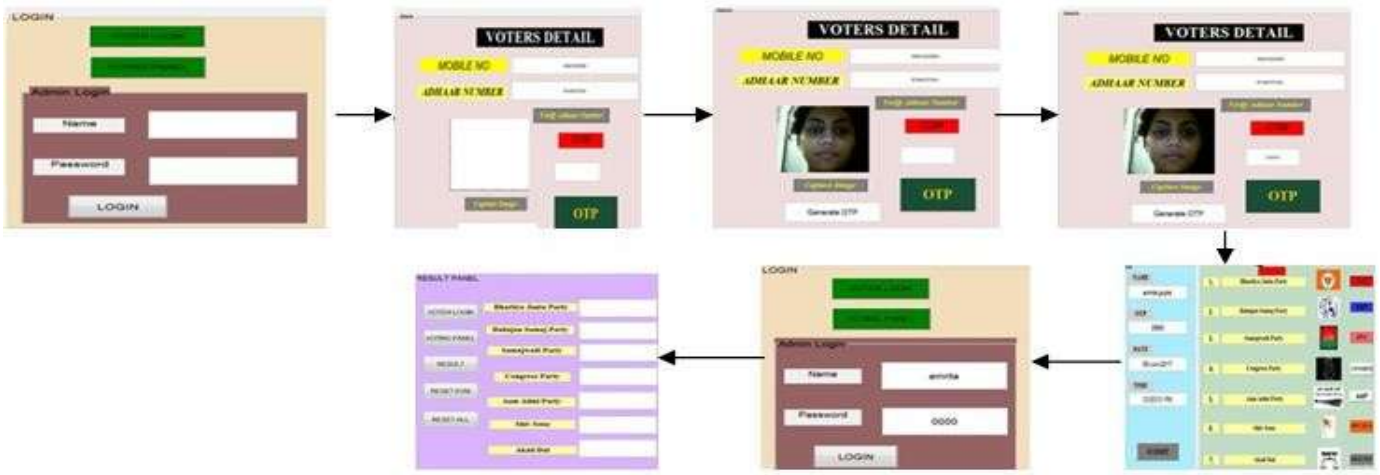


Fig 1.12:- Flow process sequence

(a) Voter login interface
(b) Voter detail input page
(c) Image capture and verification
(d) COM Port Entry Stage
(e) OTP verification and vote submission
(f) Admin login stage
(g) Result panel interface.

Discussion

The use of biometric technology in voting systems is anticipated to introduce considerable advancements in election transparency, efficiency, and security. The Voter Login Interface is used to ensure safe access to the system, with voters confirming their identities through credentials and biometric authentication, i.e., fingerprints or facial biometrics. The process removes unauthorized access and consolidates voter identification. Upon successful login, the Voter Detail Input Page confirms voter details are well recorded and vetted, excluding identity fraud, and ensuring eligible individuals only make it to voting.

For additional security, the Image Capture and Verification process is applied, in which face recognition and fingerprint scanning are utilized for voter verification. This process reduces impersonation and double voting, further tightening the electoral process integrity. Second, the OTP Verification and Vote Submission process provides an additional level of security. Voters are given a one-time password (OTP) on their registered mobile numbers, which they have to input prior to voting. This secures the process against unauthorized utilization and ensures that a voter can vote only once, and this thwarts electoral fraud.

Election officials must also ensure the security and openness of the voting process. The Admin Login Stage provides secure access to authorized officials who are responsible for supervising and managing the election system. Limited access ensures that only verified officials will be able to oversee the voting process, preventing any external interference. Finally, once the voting process is complete, the Result Panel Interface displays real-time results of the election securely. With a user-friendly and open interface, the system allows accurate counting of votes, reducing errors and tampering. This step enhances public trust in election results by ensuring votes are

counted and displayed accurately.

While biometric voting has vast advantages, challenges such as cost of deployment, privacy, and data security have to be addressed. Developing countries might face challenges in deploying biometric voting systems, requiring large capital investment and technology support. Additionally, governments must have effective cyber security protocols in place and also have in place effective legal infrastructure to protect voters' data from intrusions and abuse. Subject to overcoming these challenges, pilot schemes and phased roll-outs by 2025 could demonstrate the feasibility and effectiveness of biometric voting and result in mass take-up. In the unlikely event that it is properly integrated, biometric voting systems will revolutionize the electoral process to be more secure, transparent, and fraud-proof, thereby improving democracy in the digital era.

Conclusion

Biometric voting systems have the potential to revolutionize elections with added security, transparency, and efficiency. The integration of fingerprint and facial recognition capabilities gives accurate voter verification, eliminating fraud and tampering. The technology has the potential to greatly improve the integrity of elections, restoring the confidence of citizens in democratic processes. However, implementation logistics, privacy concerns, and security risks to data have to be considered with caution. Governments and electoral commissions have to put in place strong cyber security protocols and ethics provisions to protect the data of voters. Pilot programs and incremental roll-out may test the viability of biometric voting, but mass application will require ongoing technological advances, legal instruments, and public support. Ultimately, if done correctly, biometric voting can pave the way to a more secure and dependable electoral process, where every vote matters in determining the future of democracy.

References

- D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, "Secure Online Voting System Using Biometric and Blockchain," Advances in Intelligent Systems and Computing, vol. 1042, pp. 93–110, 2020.
- S. Agarwal, A. Haider, A. Jamwal, P. Dev, and R. Chandel, "Biometric based secured remote electronic voting system," 2020 7th International Conference on Smart Structures and Systems (ICSSS), 2020.
- K. Tyagi, T. F. Fernandez, and S. U. Aswathy, "Blockchain and Aadhaar based Electronic Voting System," Proceedings of the 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 498–504, 2020.
- S. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, "Privacy preserving E-voting cloud system based on ID based encryption," Peer-to-Peer Networking and Applications, vol. 14, pp. 2399–2409, Jul. 2021.
- S. Risnanto, Y. B. A. Rahim, N. S. Herman, and A. Abdurrohman, "E-Voting readiness mapping for general election implementation," Journal of Theoretical and Applied Information Technology, vol. 98, no. 20, pp. 3280–3290, 2020.
- T. M. A. Elven and S. A. Al-Muqorrobin, "Consolidating Indonesia's Fragile Elections Through E-Voting: Lessons Learned from India and the Philippines," Indonesian Comparative Law Review, vol. 3, no. 1, pp. 63–80, 2021.
- B. Olumide, O. Olutayo, and S. Adekunle, "A Review of Electronic Voting Systems: Strategy for a Novel," International Journal of Information Engineering and Electronic Business, vol. 12, no. 1, pp. 19–29, 2020.
- M. Khosla, "The possibility of modern India," Global Intellectual History, 2021.
- Z. Desai and A. Lee, "Technology and protest: the political effects of electronic voting in India," Political Science Research and Methods, vol. 9, pp. 398–413, Apr. 2021.
- Y. B. Hamdan, A. Sathesh, "Construction of Efficient Smart Voting Machine with Liveness Detection

Module," Journal of Innovative Image Processing, vol. 3, no. 3, pp. 255–268, 2021.

- C. Sheela and G. F. Ramya, "E-voting system using homomorphic encryption technique," Journal of Physics: Conference Series, vol. 1770, no. 1, 2021.
- A. Arora, "Election Commission of India: Institutionalising Democratic Uncertainties," Asian Affairs, vol. 52, no. 1, pp. 228–230, 2021.
- N. Kaushal and P. Kaushal, "Human Identification and Fingerprints: A Review," Journal of Biometrics and Biostatistics, vol. 02, no. 04, 2011.
- J. K. Appati, P. K. Nartey, E. Owusu, and I. W. Denwar, "Implementation of a Transform-Minutiae Fusion- Based Model for Fingerprint Recognition," International Journal of Mathematics and Mathematical Sciences, vol. 2021, pp. 1–12, Mar. 2021.
- R. S. Ghiass, O. Arandjelovic, H. Bendada, and X. Maldague, "Infrared face recognition: A literature review," The 2013 International Joint Conference on Neural Networks (IJCNN), pp. 1–10, IEEE, Aug. 2013.
- Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face Recognition Systems: A Survey," Sensors, vol. 20, p. 342, Jan. 2020.
- S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," Expert Systems with Applications, vol. 143, p. 113114, Apr. 2020.
- M. A. Bhimrao and B. Gupta, "An empirical study of dermatoglyphics fingerprint pattern classification for human behavior analysis," Social Network Analysis and Mining, vol. 13, p. 79, Apr. 2023.
- S. Jabin, S. Ahmad, S. Mishra, and F. J. Zareen, "iSignDB: A database for smartphone signature biometrics," Data in Brief, vol. 33, p. 106597, Dec. 2020.
- J. Mason, R. Dave, P. Chatterjee, I. Graham-Allen, A. Esterline, and K. Roy, "An Investigation of Biometric Authentication in the Healthcare Environment," Array, vol. 8, p. 100042, Dec. 2020.
- S. Dargan, M. Kumar, "Comprehensive survey on biometric recognition systems based on physiological and behavioral modalities," Expert Systems with Applications, vol. 143, p. 113114, Apr. 2020.
- M. Khosla, "Possibility of modern India," Global Intellectual History, 2021.
- Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face Recognition Systems: A Survey," Sensors, vol. 20, p. 342, Jan. 2020.
- T. M. A. Elven, and S. A. Al-Muqorrobin, "Consolidating Indonesia's Fragile Elections Through E-Voting: Lessons Learned from India and the Philippines," Indonesian Comparative Law Review, vol. 3, no. 1, pp. 63–80, 2021.