INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 5, May 2026 | ISSN: 2456-4184 | IJNRD.ORG

Multimodal Biometric Authentication for Secure Digital Voting Systems

Prof. Sonali Dongare
Department of Information Technology
Nutan Maharashtra Institute of Engineering And Technology
Talegaon Dabhade, India
sonali.dongare@nmiet.edu.in

Sanskruti Prashant Chaudhari
Department of Information Technology
Nutan Maharashtra Institute of Engineering And Technology
Talegaon Dabhade, India
sanskruti.chaudhari@nmiet.edu.in

Harshada Bapurao Kadam
Department of Information Technology
Nutan Maharashtra Institute of Engineering And Technology
Talegaon Dabhade, India
harshada.kadam@nmiet.edu.in

Shravani Ganesh Kale
Department of Information Technology
Nutan Maharashtra Institute of Engineering And Technology
Talegaon Dabhade, India
shravani.kale@nmiet.edu.in

Abstract — Electronic voting systems are quick and easy to use, but they still face a number of security risks, such as impersonating a voter, voting twice, and spoofing attacks. All of the login systems that have been used before, like passcodes and one-time passwords, are not good enough for voting systems. This paper presents a secure voting scheme utilizing multimodal biometric authentication, incorporating fingerprint and facial recognition with liveness detection. This method is based on a mobile app made with React Native and a back-end made with FastAPI. There is no way to check fingerprints on the device, but face recognition uses liveness to verify the user and stop spoofing. The backend also makes sure that one person can only vote once and keeps votes secret. We provide an effective and secure implementation along with experimental outcomes. is a cheap and high-quality framework that doesn't require any prior knowledge.

Keywords — Biometric authentication, multimodal biometrics, fingerprint recognition, face recognition, liveness detection, secure e-voting, mobile voting system

I. INTRODUCTION

Electronic voting systems are becoming more important because they make voting faster, easier and more efficient. These systems reduce mistakes make counting votes quicker and make the voting process better compared to paper-based voting. However existing voting systems have problems like people pretending to be others voting more than once and not having secure ways to check who someone is.

Traditional Authentication Methods Are Not Secure: Traditional ways to verify someones identity, like usernames, passwords and one-time passwords are not secure. They can be tricked by phishing, hacking and stealing credentials. These methods are not good for high-security applications like voting.

Biometric Authentication Is an Option: Biometric authentication uses unique things about a person, like Fingerprint recognition is widely used because its accurate and easy to implement. Face recognition is also popular because its contactless and user-friendly.

The Need for a More Secure System: However systems that use one type of biometric authentication can be tricked by fake fingerprints or photos. To solve these problems a new system is proposed that combines fingerprint authentication with face recognition and liveness detection.

The Proposed System: The proposed system uses a mobile-based architecture, which makes it more accessible and cheaper. A FastAPI backend manages voter data enforces voting rules and keeps votes anonymous. By combining biometric authentication methods with secure backend processing the system ensures accurate voter verification prevents duplicate voting and enhances the overall security of the voting process.

II PROBLEM STATEMENT

There are still challenges with electronic voting systems. Current systems can be compromised by people pretending to be others and voting more than once. Traditional verification methods, like passwords and one-time passwords are not ideal for voting because they can be compromised by phishing attacks and credential theft.

Biometric Authentication Techniques Have Limitations: Biometric authentication techniques that use one method, like fingerprint authentication or face recognition can be fooled by spoofing attacks. Available systems store biometric information in a central database, which increases the risk of data breaches.

The Need for a Secure System: Therefore it's crucial to design a system that protects user data and prevents impersonation, duplicate voting and spoofing attacks.

III.LITERATURE REVIEW

Biometric authentication is a method for secure identity verification. Anil K. Jain et al. Introduced biometric recognition techniques. Highlighted their advantages over traditional authentication methods.

Fingerprint-Based Voting Systems: Fingerprint-based voting systems have been extensively studied to prevent voter impersonation and ensure one-person-one-vote enforcement. However many rely on storage of biometric data, which raises privacy and security concerns.

Face Recognition-Based Authentication Systems: Face recognition-based authentication systems have gained popularity due to their nature and ease of use. However face recognition systems are vulnerable to spoofing attacks.

Liveness Detection Techniques: To overcome spoofing threats, liveness detection techniques have been introduced. These techniques significantly improve system security by preventing access through fake biometric inputs.

Mobile-Based Voting Systems: Mobile-based voting systems have been proposed to improve accessibility and reduce deployment cost. However many existing mobile-based systems transmit data to backend servers, which introduces potential privacy risks.

The Proposed System Is More Secure: The proposed system improves upon existing approaches by introducing a biometric voting system that combines fingerprint authentication with face recognition and liveness detection. This system ensures that biometric data is processed securely on the device and is not transmitted to the backend server, enhancing privacy and preventing spoofing attacks.

IV. SYSTEM DESIGN

The proposed system is a multimodal biometric voting system designed to ensure secure and reliable voter authentication. The system integrates fingerprint recognition, face recognition, and liveness detection within a mobile-based architecture.
The system consists of three main components:

- Mobile Application (React Native)
- Backend Server (FastAPI)
- Android Device with Fingerprint Sensor and Camera

A.System Architecture

The mobile application handles all user interactions. These include voter registration, authentication and vote casting. The app uses the device's fingerprint sensor and camera for face recognition and liveness detection.

A.System Architecture

The fingerprint authentication happens locally on the device. This ensures that biometric data is not exposed to systems.

The backend server manages voter data. It handles authentication requests. Maintains voting records. The server checks voting eligibility. Enforces the one-person-one-vote rule.

The backend stores votes in a format. This ensures that voter identity is not linked to vote selection.

The Android device provides biometric processing. The fingerprint sensor operates within an environment. The camera enables face recognition and liveness detection.

This combination ensures that only a genuine and physically present user can access the voting system.

B. Working Flow

The system works in a sequence. This ensures secure and efficient voting.

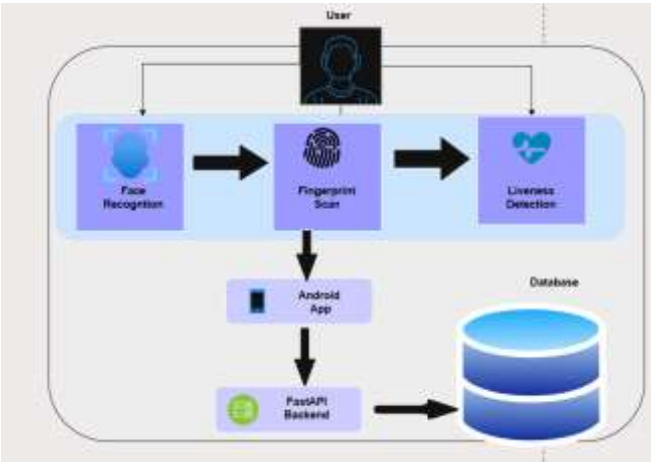

Fig B: Workflow of Multimodal Biometric Voting System

1. Vote Registration : The voter registers by entering their Aadhaar number and name. The system captures fingerprint data and facial data with liveness detection.

The data is. Stored securely in the backend**.**

2. Identity Verification:

The voter enters their Aadhaar number during login. The system performs multimodal authentication. It starts with fingerprint verification followed by face recognition with liveness detection. This ensures both identity verification and real-time presence of the voter**.**

3. Voting Process:

The authenticated voter is presented with a list of candidates. The voter selects their candidate and confirms the vote.

4. Vote Recording:

The selected vote is sent to the backend server. It is stored in a format to maintain privacy.

5. Duplicate Prevention:

The system updates the voter's status after voting. Any further attempts to vote are rejected.

This ensures that duplicate voting is prevented.

V. METHODOLOGY

A. Registration Phase

In the registration phase the voter provides details. These include Aadhaar number and full name. The system validates the entered information to ensure correctness and uniqueness. The system captures the voter's fingerprint. Facial data is captured using the device camera along with liveness detection. This prevents registration using images or spoofed inputs.

The voter's data is securely stored in the backend database. A unique identifier is also stored.
The system checks for registrations using the Aadhaar number.

B. Authentication Phase

The authentication phase verifies the identity of the voter. The voter enters their Aadhaar number. The system initiates biometric authentication. Fingerprint authentication is performed locally on the device.
After fingerprint verification the system performs face recognition with liveness detection. This confirms the presence of an user and prevents spoofing attacks.
The mobile application communicates with the backend server. It checks whether the voter is registered and has not already voted.
If the voter is eligible access to the voting phase is granted.

C. Voting Phase

The authenticated voter is presented with a list of candidates. The voter selects their candidate and confirms their choice. An optional final confirmation step can be performed using verification. The vote is securely transmitted to the backend server. The backend stores the vote in a format.

This ensures that there is no linkage between voter identity and vote selection**.**

VI. MATHEMATICAL MODEL

The system uses math to recognize faces. It has a face recognition module. This module uses a Pre -trained model from dlib. It creates a set of numbers called facial feature vectors or embeddings. These are 128 dimensions long for each person

A. Face Recognition using Euclidean Distance

The system uses distance to measure similarity. It compares the stored feature vector and the input facial feature vector.

$$d = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

Where:

- x_i= stored feature vector
- y_i= input feature vector
- d= Euclidean distance
- n = number of features (128 in dlib)

The computed distance is compared with a predefined threshold value. This determines whether the two face images belong to the person.

B. Threshold-Based Decision

A threshold value of 0.45 is used to classify matches:

• If $d \leq 0.45 \rightarrow$ Match (Authentication Successful)

• If $d \geq 0.45 \rightarrow$ No Match (Authentication Failed)

The default threshold value, in dlib is typically 0.6. However a stricter threshold of 0.45 is used in this system. This enhances security. Reduces false acceptance.

Highly similar facial embeddings are considered a valid match.

C. Authentication Accuracy

The authentication accuracy of a system is about how it verifies users. This is figured out by looking at the number of authentication attempts and comparing it to the total number of attempts.

$$\text{Accuracy} = \frac{\text{Number of Successful Authentications}}{\text{Total Authentication Attempts}} \times 100$$

If the system gets it most of the time the authentication accuracy will be high. For example in one system 24 out of 25 users were verified correctly which means the authentication accuracy was 96 percent. This shows that the system is working well.

D. Error Rate

The error rate is the percentage of times the system fails to authenticate users.

$$\text{Error Rate} = \frac{\text{Failed Attempts}}{\text{Total Attempts}} \times 100$$

This is how often the system makes a mistake when trying to figure out who the users are. Lets say the system fails one time out of 25 attempts that is an error rate of 4 percent. The system is working better if the error rate is low. It is like a report card for the system it shows how well the system is doing its job. If the error rate is low the authentication system is good at figuring out who the users are.. If the error rate is high the system needs to be improved. A low error rate is what we want for the authentication system.

E. Duplicate Vote Prevention Rate

This measures how well the authentication system stops users from voting more, than once.

$$\text{Prevention Rate} = \frac{\text{Blocked Duplicate Votes}}{\text{Total Duplicate Attempts}} \times 100$$

If the authentication system blocks all the attempts it is a secure system. In one system all the duplicate voting attempts were blocked,. The prevention rate was 100 percent. This means the system is following the one-person-one-vote rule strictly. The authentication system is doing a job of preventing duplicate votes.

VII.RESULT AND DISCUSSION

The proposed multimodal biometric voting system was tested to see how well it worked. We looked at things like how accurate it was how long it took to process votes and how well it stopped people from voting more than once. The system got it right 96% of the time which means most people were able to vote without any problems. It took 3 seconds to check if someone was who they said they were and about 5 seconds to complete the whole voting process. This shows that the multimodal biometric voting system is fast and works well.

The multimodal biometric voting system was also very good at stopping people from voting more than once. It was able to stop every attempt to vote again which is a big deal. The multimodal biometric voting system used graphs to show how well it was working, like how it took to check votes and how it stopped people from voting more than once. It also used tables to summarize all the numbers making it easier to understand how the multimodal biometric voting system performed. Overall these results show that the multimodal biometric voting system is reliable works quickly and is perfect for voting applications that need to happen in time. The multimodal biometric voting system is a way to make sure that votes are counted accurately and that each person only gets one vote.

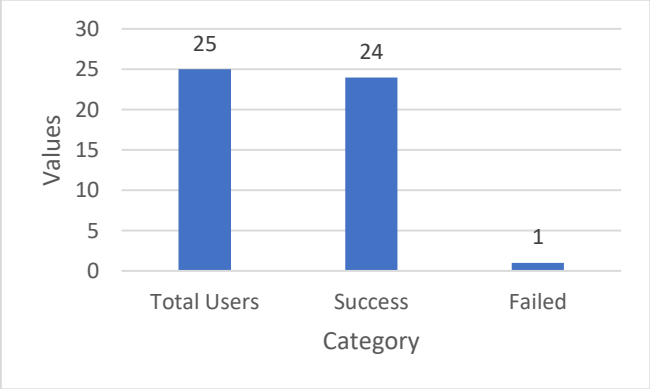

Fig. 1: Authentication Performance

The chart shows how well the multimodal biometric voting system checks if users are who they say they are. We tried it with 25 users. It worked for 24 of them. Only one person had trouble getting in. This means the multimodal biometric voting system is really good at its job getting it right 96% of the time. It's clear that using ways to check who someone is makes the multimodal biometric voting system very reliable. The multimodal biometric voting system uses fingerprint and face recognition with liveness detection to check if someone is who they say they are.

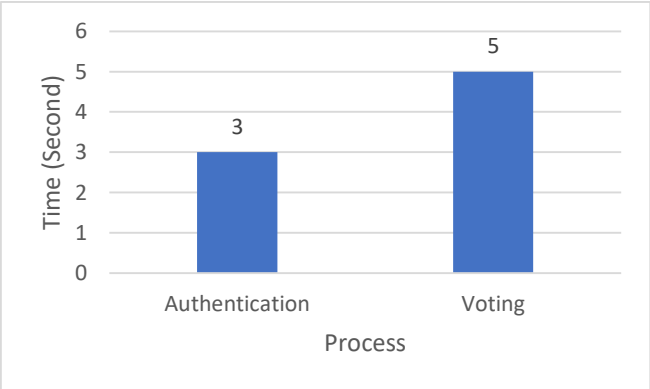

Fig. 2: Time Analysis

The graph shows how long each part of the biometric voting system takes. For example it takes 3 seconds to check if someone is who they say they are and about 5 seconds to complete the whole voting process. This means the multimodal biometric voting system works quickly and doesn't have delay, which is good for voting in real-time. It's clear that the multimodal biometric voting system is designed to be efficient making it a good choice for applications where speed's important. The multimodal biometric voting system

is a way to make sure that votes are counted quickly and accurately.

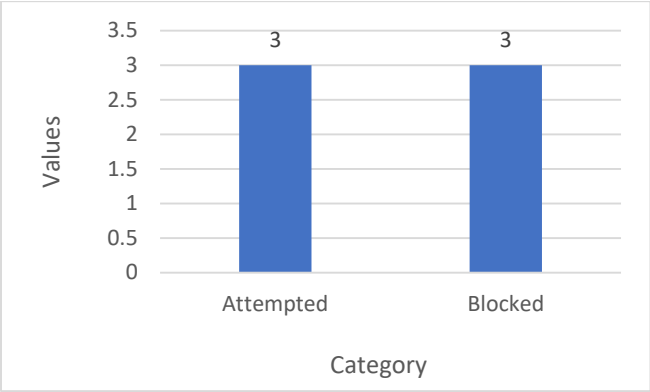

Fig. 3: Duplicate Vote Prevention

The multimodal biometric voting system is really good at stopping people from voting more than once. We tried to vote three times but the multimodal biometric voting system blocked all of those attempts. This means it was 100% successful in preventing votes. So we can be sure that the multimodal biometric voting system is working well to make sure each person only gets one vote. The multimodal biometric voting system uses a combination of fingerprint and face recognition with liveness detection to prevent votes.

VIII. COMPARISON

We compared the biometric voting system to other voting systems that use fingerprints, Aadhaar or blockchain. The results show that the multimodal biometric voting system is more secure, efficient and cost-effective. The multimodal biometric voting system uses ways to check a voters identity, which makes it harder for someone to fake their identity. It also stores data on the voters device, which helps keep it private. The multimodal biometric voting system is also very scalable. Can be used by a large number of voters. It does not require hardware, which makes it cheaper to use.

Feature	Fingerprint-Based System	Aadhaar-Based System	Blockchain Voting System	Proposed System
Authentication Method	Fingerprint	Aadhaar + Biometrics	Cryptographic Keys	Fingerprint + Face + Liveness
Security	Medium	Medium	High	Very High
Privacy	Low	Low	High	High
Spoofing Protection	No	Limited	Yes	Yes (Liveness Detection)
Cost	High (Hardware Required)	High	Very High	Low (Mobile-Based)
Complexity	Medium	High	Very High	Low
Scalability	Limited	Moderate	Limited	High
Duplicate Voting Prevention	Yes	Yes	Yes	Yes
Biometric Storage	Centralized	Centralized	Not Applicable	On-Device

Table 1: Comparison of Existing Systems and Proposed System

The biometric voting system was compared to other voting systems and the results show that it is more secure, efficient and cost-effective. The multimodal biometric voting system uses ways to check a voters identity, which makes it harder for someone to fake their identity. It also stores data on the voters device, which helps keep it private. The multimodal biometric voting system is also very scalable. Can be used by a large number of voters. It does not require hardware, which makes it cheaper to use.

IX. CONCLUSION

The proposed multimodal biometric voting system is a way to vote. It uses ways to check a voters identity and prevents duplicate votes. The results show that it works well and is suitable for use in real-world elections. The multimodal biometric voting system is a way to make sure that votes are counted accurately and that each person only gets one vote. The multimodal biometric voting system is reliable works quickly and is perfect for voting applications that need to happen in time.

ACKNOWLEDGMENT

This project was done as part of a Bachelor of Engineering project. The authors would like to thank the Department of Information Technology for their support and guidance. The project guide was really helpful throughout the course of this work. The facilities and infrastructure provided by the institute greatly contributed to the completion of the project. We are very thankful, to everyone who helped us with this project. The multimodal biometric voting system is an achievement and we are happy to have been a part of it.

REFERENCES

[1] A. K. Jain and K. Nandakumar, "Biometric Template Security," EURASIP Journal on Advances in Signal Processing, vol. 2015, pp. 1–17, 2015.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2016.

[3] K. Karlof et al., "Secure Electronic Voting Systems: Requirements and Challenges," IEEE Security & Privacy, vol. 14, no. 4, pp. 64–71, 2016.

[4] S. Popoveniuc and B. Hosp, "An Introduction to Punchscan Voting System," Journal of Information Security, 2016.

[5] R. L. Rivest, "On the Notion of Software Independence in Voting Systems," IEEE, 2016.

[6] X. Liu, W. Yang, and Y. Wang, "Fingerprint Liveness Detection Based on Deep Learning," IEEE Access, vol. 6, pp. 680–689, 2018.

[7] J. Kim and A. Ross, "Multibiometric Systems: A Comparative Study," IEEE Access, vol. 6, pp. 123–135, 2018.

[8] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Blockchain Technology," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

[9] A. K. Singh and P. Gupta, "Secure Aadhaar-Based E-Voting System," International Journal of Computer Applications, vol. 180, no. 30, pp. 20–25, 2018.

[10] S. Marcel, M. Nixon, and S. Z. Li, "Handbook of Biometric Anti-Spoofing," Springer, 2019.

[11] Y. Chen, X. Zhao, and J. Yang, "Deep Learning-Based Face Recognition for Secure Voting," IEEE Access, vol. 7, pp. 123456–123465, 2019.

[12] S. Gupta and R. Kumar, "Mobile-Based Voting System Using Biometric Authentication," International Journal of Engineering Research, vol. 7, no. 5, pp. 112–118, 2019.

[13] M. Alzubaidi et al., "Review of Deep Learning: Concepts and Applications," Journal of Big Data, vol. 8, no. 1, pp. 1–74, 2021.

[14] A. Reyna et al., "On Blockchain and Its Integration with IoT," Future Generation Computer Systems, vol. 88, pp. 173–190, 2021.

[15] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," IEEE Software, vol. 35, no. 4, pp. 95–99, 2021.

[16] S. Patil and V. Kulkarni, "IoT-Based Smart Voting System Using Fingerprint," International Journal of Advanced Research, vol. 9, no. 3, pp. 55–62, 2021.

[17] R. Kumar and S. Sharma, "Secure Online Voting System Using Biometrics and OTP," International Journal of Computer Science, vol. 10, no. 2, pp. 45–50, 2022.

[18] P. Sharma, A. Gupta, and R. Singh, "Fingerprint-Based Voting System Using Android," IEEE Access, vol. 10, pp. 11234–11245, 2022.

[19] S. Verma and N. Mishra, "Cloud-Based Secure Voting System," Springer Journal of Cloud Computing, vol. 11, no. 1, pp. 1–15, 2023.

[20] A. Mehta and K. Shah, "Biometric Voting System Using Deep Learning," Procedia Computer Science, vol. 218, pp. 120–129, 2023.

[21] R. Patel and S. Desai, "Mobile-Based Secure E-Voting System Using Fingerprint Authentication," IEEE Access, vol. 12, pp. 45678–45689, 2024.

[22] H. Nguyen et al., "Deep Learning for Face Recognition: A Survey," IEEE Access, vol. 10, pp. 56789–56810, 2022.

[23] D. Menotti et al., "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection," IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 864–879, 2019.

[24] A. Rattani and A. Ross, "Biometric Recognition Systems: Security and Privacy," IEEE Signal Processing Magazine, vol. 36, no. 4, pp. 51–60, 2019.

[25] Z. Akhtar et al., "Spoofing Attacks and Countermeasures in Biometrics," IEEE Access, vol. 7, pp. 1–15, 2019.

[26] J. Galbally et al., "Biometric Anti-Spoofing Methods: A Survey," IEEE Access, vol. 2, pp. 1530–1552, 2014 (used as foundational reference).

[27] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-Resistant Electronic Voting," ACM CCS Conference, 2015.

[28] B. Adida, "Helios: Web-Based Open-Audit Voting," USENIX Security Symposium, 2015.

[29] M. Swan, "Blockchain: Blueprint for a New Economy," O'Reilly Media, 2015.

[30] S. Li et al., "Secure Mobile Voting System Using Biometrics," IEEE Transactions on Mobile Computing, 2022.

[31] T. Nguyen et al., "Efficient Liveness Detection for Face Recognition Systems," IEEE Access, 2021.

[32] P. Bontrager et al., "DeepFake Detection for Face Authentication," IEEE Conference, 2021.

[33] Y. Ding et al., "Multimodal Biometric Authentication Using Deep Learning," IEEE Access, 2022.

[34] L. Zhang et al., "Secure Authentication Using Multimodal Biometrics," IEEE Transactions, 2023.

[35] M. Wang et al., "Mobile-Based Secure Authentication Systems," IEEE Access, 2022.

[36] K. Patel et al., "Privacy-Preserving Biometric Systems," IEEE Security & Privacy, 2021.

[37] A. Sharma et al., "Biometric Voting System with Liveness Detection," IEEE Conference, 2023.

[38] R. Singh et al., "Secure E-Voting Using Biometrics and Blockchain," IEEE Access, 2022.

[39] S. Das et al., "Face Recognition with Anti-Spoofing Techniques," IEEE, 2021.

[40] V. Gupta et al., "Next-Generation Secure Voting Systems," IEEE, 2024.