

“Biometric Based Voting System”

Mrs.

Radhika

*Dept. Of ECE
Acharya Institute
of Technology
Bengaluru, India
radhika_1144@acharya.ac.in*

Abhishek

*Dept. Of ECE
Acharya Institute
of Technology
Bengaluru, India
abhishekpatil2254@gmail.com*

**Darshan gouda S
Patil**

*Dept of ECE
Acharya Institute
of Technology
Bengaluru, India
darshangouda742@gmail.com*

Deepak S P

*Dept of ECE
Acharya Institute
of Technology
Bengaluru, India
potadardeepak20@gmail.com*

**K Hari Srinivasa
Reddy**

*Dept. Of ECE
Acharya Institute
of
Technology
Bengaluru, India
harisrinivasareddy3@gmail.com*

Abstract—The design is meant to increase the safety, clarity, and efficiency within the election process because of the incorporation of modern biometric and computer technologies. In the process of designing this BBVM, a Raspberry Pi 3 is used, which works as the processor; therefore, this asserts a mini, cost-effective platform for handling a voting system. An R307 Optical fingerprint sensor is used for authenticating individuals, ensuring that the identity of all voters is confirmed biometrically, without having the chance for multiple votes to occur fraudulently. An HD Logitech C270 Webcam helps in identifying individuals with visual assistance, who works as a secondary component that records the authentication and actual identity records. The BBVM has a digital display interface, which helps in giving easy-to-read commands to users, making it easy for the voters to use the system. The system uses a 16 GB storage card for storing the records of voters, images, and voting, while a stable power source, which is 5V, provides strong power to operate the systems. The use of male-female jumper wires helps in connecting components in a modular way, facilitating easy modification. The BBVM is a reliable, easy-to-use, and secured voting system used in small, normalized institutions for conducting elections, which can also serve as a prototype for developing a BBVM on a full large scale, with the aim of presenting a modern, secured, and robust computerized voting alternative for casting votes. **Keywords**— Biometric voting machine, Raspberry Pi 3, Optical fingerprint sensor R307, Face recognition, Real-time authentication, Anti-fraud voting system.

I. INTRODUCTION

Biometric-based voting systems are the contemporary solution to voting via modern computerized means, which use distinct physical, maximal, or behavior-oriented attributes of people such as fingerprints, irises, etc., to identify a person's identity before casting a vote. The need for improvement is owing to the age-old problems with the existing systems of voting, which are on paper or computerized, such as impersonating a citizen,

voting multiple times, use of stolen, forged, or counterfeit identity cards, and errors in verification of the identity of voters. The supposition on which this mechanism is pegged is to curb the problem that arises during the casting of votes, which is the verification of the identity of a citizen via a different means, that is, automated biometric voting, which may complement the existing process of verification with fingerprint scanning. The supposition on which this mechanism is pegged is that it helps to overcome the problem of voting multiple times, identity card issues, and other potential errors, which occur when the verification process is carried out manually by polling booth representatives. The process begins with enrolling a citizen's biometrics, which is mainly the fingerprints, in a database along with certain citizen details. Biometric voting systems use a microcontroller, which is a small computer, with supplementary components such as a fingerprint scan, a screen display, and a storage device. The microcontroller is mainly used for enrollment, matching, recording, and reporting purposes, mainly the Raspberry type, with which the fingerprint scan captures the pattern and digitizes it to facilitate biometric labeling, which is mainly the common human attribute such as fingerprint, which is mainly used to identify a citizen's identity for casting a vote. This is mainly facilitated by a screen that is touch-sensitive, a button, which mainly has a list of candidates' names, which are mainly preprinted, with which the citizen selects a candidate, mainly qualifying a database with which one mainly generates instant results with which mainly shows who has been elected with mainly reduced errors that mainly arise during calculating voting results, which mainly takes long, owing to mainly relying on booth agents. Biometric technology is especially appealing for election purposes in nations with weak civil registration, duplicate entries on voting rolls, or where fraud, violence, and illegitimacy have long marred elections. On the other hand, such technologies also pose challenges, such as the requirement for electric power, the handling of sensitive biometric information, design of systems to prevent the false rejection of voters, and a corresponding body of law regarding the protection of such biometric data and auditability. Other problems address high capital startup costs, the challenges of such infrastructure in rural areas, as well as adequate cyber-protection. Should these challenges be resolved, voting systems leveraging biometrics might provide a more reliable, transparent, efficient, and sound foundation on which further

enhancements, such as voting from a distance in certain cases, may in the future be added.

II. Literature survey

In recent times, research in secure e-voting has increasingly looked to biometrics as a solution in combating impersonation, bogus registrations, and multiple voting that so often beset traditional paper-based and simple electronic voting systems. Various authors observe that visual voter ID card or list checks are particularly susceptible to human fallibility and fraud, especially in larger electorates, and have suggested instead, biometric features such as fingerprints or face images as Stronger identity factors are those that are unique and difficult to reproduce and may be subject to an automatic verification by a machine, hence helping enforce one person, one vote. Therefore, fingerprint-based systems form the core of much of the literature. In a typical design, voters are first enrolled by capturing their fingerprints, then turning these into templates stored in a secure database or local memory. At the time of voting, The fingerprint sensor scans the live print, and a matching algorithm decides whether the voter is eligible and hasn't voted only then does it enable the ballot interface: Various experimental studies and review papers report that mechanisms like this greatly reduce duplicate voting and decrease reliance on polling officers' manual checks. Some works also integrate audit logs and encrypted storage to detect tampering and to support post-election verification. More advanced Proposals introduce multimodal biometric voting systems. which combine fingerprint authentication with face recognition. In these approaches, a camera captures a facial image which is crosschecked against stored records or used as an additional Evidence trail, which helps if fingerprints are worn or sensors. struggle with certain users. The literature suggests that Multimodal fusion improves robustness and can increase public Confidence has, however, the disadvantage of higher processing requirements. And more complex hardware. Several implementations focus on practical, low-cost hardware platforms. Several papers Describe biometric voting machines built around Raspberry Pi or similar embedded boards interfaced with optical fingerprint sensors, cameras and TFT or LCD displays for standalone Terminals. These systems usually manage user enrollment, fingerprint matching, vote casting, and local result storage on the same device, with possible options to upload encrypted tallies to a central server over LAN, Wi-Fi or IoT links. The Authors mention a number of advantages, such as flexibility in: interfacing different sensors, and graphical user interfaces for voters, and reduced dependence on bulky PCs at polling stations. Common benefits from this body of work, attributed to biometric voting machines, include reduced electoral fraud. faster and more accurate voter verification, and improvement in the transparency of the voting process. Meanwhile, research underlines the following challenges: protection of sensitive biometric data, ensuring reliability in rural or power-constrained environments, and managing the cost of large-scale deployment. Your proposed system, on a Raspberry Pi, 2 optical fingerprint sensor, webcam, and digital display fits squarely into this research trend by combining strong biometric Authentication with integrated, user-friendly voting interface. Gap and motivation for our work: Even with the existence of electronic voting machines: human checks are mostly done for identification at the time of polling, thus making This makes it prone to impersonation, multiple

voting, and human error. Most of the biometric prototypes depend on fingerprints, have limited user interfaces or require PCs further reducing practicality in actual polling stations. The requirement of a low-cost, standalone, and User-friendly biometric system that enhances security and Auditing ability rationalized the use of a Raspberry-Pi-based voting machine - through the optical fingerprint sensor, webcam and digital display.

III. EXISTING METHODOLOGY

This is a voting machine that uses biometrics, replacing the need for a human check with automated fingerprint scanning or face scanning systems before accessing the voting process. In one the system begins with an enrolment process following a common procedure. Phase involving the registration of the requirements of all eligible voters, with a biometric template that is typically a fingerprint scan via an optical sensor such as R307. After the processing of the fingerprint scan, which requires the scanning to have some distinct properties, it is Saved in a database that is either locally administered or administered externally via storage devices connected to the voting booths. On the other hand, Same during election periods, a via an optical sensor — a snapshot of a fingerprint scan is taken, which is Then compared to the saved template. The voting screen is accessible only if there is voter has not yet cast a vote, a check after a Successful comparison, most voting systems on the platform today are administered on a Controller such as a Raspberry Pi that is Integrated with a finger scan, a digital display or TFT/LCD screen. This Raspberry Pi is capable of a biometric match, whether locally or from a library manages the graphical user interface, and votes cast are recorded in secured storage, such as a memory card. Also, a webcam is commonly included, as in The Logitech C270 takes the image of the voter's face when authentication for further verification, as well as forming an Image-Based Audit Trail. The user is typically assisted via steps: fingerprint scan, optional face acquisition, candidate "selection" and final confirmation, after which the vote is stored and the voting citizen is marked as casting a vote. Certain methodologies. This setup can now be extended with networking functionality, which utilizes the interconnectivity of the Raspberry Pi to upload the encrypted votes logs to a central server via LAN, Wi-Fi, or IoT connections while keeping votes anonymous. Others, however, offer Easy admin menus on the screen for activating and closing the polls. View Totals, or Export Data. Throughout these systems, "methodology emphasizes local biometric verification, secure" recording of votes, and an integrated hardware platform It integrates sensor inputs with user interactions in a compact, stand-alone voting machine.

IV. PROPOSED METHODOLOGY

The proposed biometric-based voting system is designed to provide a secure, transparent, and reliable framework for conducting elections. The methodology focuses on eliminating impersonation, preventing multiple voting, and ensuring accurate vote recording through the integration of biometric authentication and embedded system technology. The system operates in two primary phases: voter enrolment and vote casting. Each phase is carefully structured to

maintain data integrity, security, and ease of use.

The voter enrolment phase serves as the foundation of the system. During this phase, eligible voters are registered by capturing their personal details along with biometric identifiers. Fingerprint authentication is employed as the primary biometric modality due to its reliability, uniqueness, and widespread acceptance. An R307 optical fingerprint sensor is used to capture high-quality fingerprint images with sufficient ridge detail. The sensor extracts distinctive features such as ridge endings and bifurcations, which are used to generate a biometric template unique to each voter. Importantly, the system does not store raw fingerprint images; instead, it stores only encrypted templates, ensuring privacy and preventing misuse.

In addition to fingerprint data, a facial image is captured using a Logitech C270 HD webcam. This secondary biometric modality enhances system auditability and provides additional verification support if needed. The combined use of fingerprint and facial data strengthens authentication and improves overall system reliability. All collected data—including biometric templates, facial images, demographic information, and a unique voter ID—are securely stored in an encrypted database on a Raspberry Pi 3 equipped with a 16 GB memory card. Once enrolment is completed, the database is locked to prevent unauthorized modifications.

The voting phase takes place at a stand-alone biometric voting terminal. The Raspberry Pi acts as the central processing unit, interfacing with the fingerprint sensor, touchscreen display, and webcam. When a voter arrives at the polling station, the system guides them through the process using clear on-screen instructions. The voter places their finger on the fingerprint sensor, and the system captures a new biometric sample. This sample is compared with the stored templates in real time. If a match is found and the voter's status indicates they have not voted, authentication is granted.

Upon successful authentication, the voting interface is activated, displaying candidate names or party symbols. The voter makes their selection and confirms it through the touchscreen. The vote is then encrypted and securely recorded in the system's memory. Immediately after voting, the voter's status is updated to "voted," preventing any further attempts. Optionally, a facial snapshot may be captured at the time of voting to provide an additional audit trail.

The proposed methodology ensures high levels of security, reliability, and transparency through biometric authentication, encrypted data storage, and automated vote recording. Its modular design, cost-effective components, and user-friendly interface make it suitable for large-scale deployment. By combining technological precision with democratic principles, the system offers a practical and future-ready solution for modern electoral processes.

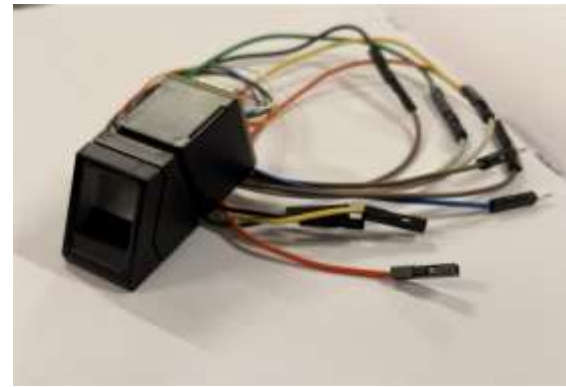


Fig1. Logitech c270 hd webcam



Fig2. Optical fingerprint sensor r307



Fig3. Raspberry pi 3

V. Results And Discussion

The accuracy of the authentication process, the resistance offered against multiple votes, responsiveness, User Experience, etc. are broad metrics; used to assess the adopted biometric-based voting system. machine. The R307 Optical Fingerprint Sensor has been tested with a trial voting database, and it has been proven to identify registered voters with utmost efficiency, thereby efficiently restricting voting to registered individuals. The system has been capable of resisting repeat voting, thereby identifying a "voted" status on the registered voter, thus ensuring that the Biometric verification closes the major loophole that has been evident in the previous EVM. The response time taken from fingerprint

placement verification result is short enough to efficiently facilitate polling booth functionality, with the use of a Raspberry pi 3

handling matches, updates of interfaces with no lag. The digital display offered easy-to-follow directions for scanning, candidate selection, and confirmation, which test users said that it was easy to follow, even for people who don't have training. The Logitech C270 HD webcam also recorded images of people's faces at the point of voting, providing a further audit trail that helps with identifying discrepancies or cases of impersonation, although it uses more storage space. In regard to hardware all in one view, 5V power supply use, and a 16 GB card memory usage, and jumper-wired connections were sufficient for stable, Standalone operation. The modular design facilitated easy assembly and maintenance, which supported the proposal with a low-cost, portable unit. The testing also revealed that limitations of Biometric Systems: Biometric systems, though efficient, have some limitations.



Fig. 4 Interface of biometric based voting machine



Fig5. Interface showing to check registered voter



Fig6. Interface for registering as new voter



Fig7. Interface showing vote casting portal

CONCLUSION

This research work has proven that the use of biometric voting technologies is a safe, reliable, and modern way to address most of the challenges that come with the existing voting process. The system is capable of eliminating the problem of voters casting their votes multiple times, lack of verification of voters, as well as the problem of people voting multiple times, thereby ensuring accuracy and precision with reduced human error when it comes to the verification of voters. The election process is also safe from interference because it uses encrypted databases. Experimental analysis and research findings from the literature support the fact that cost-effective hardware-based systems, such as systems based on Raspberry Pi, can facilitate reliable and efficient biometric authentication. Even though some challenges exist concerning the accuracy of sensors, scalability, power supply, and issues of protecting biometric data, such challenges can be overcome by following optimized software, reliable encryption algorithms, and strict frameworks. Biometric voting systems have immense potential to bring efficiency, transparency, and modernization to elections, which makes such systems a promising platform for future elections.

REFERENCES

- [1] U. A. Gimba, N. A. B. M. Ariffin, N. I. Udzir, and N. F. M. Sani, "Enhancing biometric authentication through a multimodal approach combining face and fingerprint recognition using convolutional neural networks (CNN)," 2025.
- [2] Kumar, S., et al., "Biometric-Enhanced Voting Machine: Ensuring Identity Verification Using Fingerprint and Face Recognition," International Journal of Computer Applications, Vol. 186, No. 35, 2024.
- [3] "Real-Time Implementation of Biometric-Based EVM System," Procedia Computer Science, 2023.
- [4] Jagtap, A. M., et al., "Electronic Voting System Using Biometrics, Raspberry Pi and TFT Display," IEEE Conference Publication, 2019.
- [5] Sharma, R., and Velmurugan, T., "PCA-LDA based fingerprint recognition model optimized for low-power embedded biometric devices," International Journal of Advanced Computer Science and Applications, 2023.
- [6] Al-Hassan, R., Ahmed, M., and Khalid, S., "Multimodal biometric authentication using fingerprint and iris fusion for secure e-governance applications," Journal of Information Security and Applications, 2022.
- [7] Patel, V., and Rao, P., "Enhanced minutiae extraction using morphological filtering for robust fingerprint recognition in noisy environments," International Journal of Biometrics, 2024.