e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

ENHANCED ELECTRONIC VOTING MACHINE USING MINUTIAE-BASED BIOMETRIC AUTHENTICATION FOR SECURE VOTER VERIFICATION

Dr. Amudha G*[1], Ashwin V*[2], Aaziz Mohamed A*[3], Sadhu Venkata Srinivasulu S*[4]

*[1,2,3,4]Department Of Computer Science And Business Systems, RMD Engineering College, India.

ABSTRACT

This paper introduces a secure Electronic Voting Machine (EVM) integrated with Aadhaar number verification and fingerprint biometric scanning to enhance the integrity of the voting process. Utilizing biometric authentication and unique identity verification through Aadhaar, this system is designed to prevent fraudulent voting and ensure only registered voters can participate. The approach incorporates database management for secure data storage, biometric matching algorithms for accurate fingerprint recognition, and microcontroller-based processing to streamline authentication. This combination of Aadhaar verification and biometric security enhances reliability, making it a robust solution for secure and transparent electronic voting systems.

To strengthen the security and reliability of voting systems, this project addresses the critical need for fraud prevention and voter identity verification through a combined Aadhaar-based authentication and fingerprint biometric approach. Traditional voting systems face challenges with impersonation and duplicate voting, which can compromise election integrity. By integrating these two forms of authentication, this electronic voting machine (EVM) model provides a unique dual-layer security solution, ensuring only eligible voters can participate and preventing multiple votes by the same individual. This innovative system, designed for scalability, offers enhanced security and transparency, making it suitable for adoption in large-scale elections at regional or national levels. The proposed EVM demonstrates how advanced identity verification technologies can transform the voting process, paving the way for future applications in secure electoral systems globally.

I. INTRODUCTION

The integrity and reliability of the voting process are fundamental to the democratic system, yet traditional voting methods often face challenges related to security, accuracy, and accessibility. In response, electronic voting machines (EVMs) have been introduced to improve efficiency and reduce human error. However, issues like voter impersonation and multiple voting by the same individual persist, necessitating more advanced solutions.

This project introduces an innovative Electronic Voting Machine (EVM) that integrates Aadhaar-based identity verification with fingerprint biometric scanning to enhance election security and prevent fraudulent activities. Aadhaar, a unique identification system widely used in India, provides a robust platform for verifying voter identity. By incorporating fingerprint biometrics, the system ensures that each vote is cast only once by an authenticated individual, effectively eliminating the possibility of multiple votes and voter impersonation.

The proposed Electronic Voting Machine (EVM) system integrates Aadhaar-based verification and fingerprint biometric authentication to enhance voter identification and resolve the shortcomings of traditional voting systems. The key components of the system are as follows:

Aadhaar Verification:

At the time of voter registration, each individual provides their Aadhaar number, which serves as a unique identifier. The Aadhaar database, which contains both demographic and biometric data (including fingerprints), is used to verify the voter's identity securely.

Fingerprint Biometric Authentication:

On election day, the voter’s fingerprint is captured using a fingerprint scanner. This biometric data is then compared with the fingerprint previously stored in the database during the registration phase, ensuring that the voter’s identity is accurately verified.

Database Management:

A secure and encrypted database is used to store the Aadhaar number and fingerprint data of each registered voter. The database is designed to prevent unauthorized access or tampering, ensuring that voter information remains secure and accurate.

One Vote per Person:

Once a voter has successfully cast their vote, their Aadhaar number is flagged as "voted" in the system. This prevents any subsequent voting attempts by the same individual, as the system tracks the voting status of each registered voter to enforce the one-person-one-vote rule.

Real-Time Updates:

Voter authentication and voting records are updated in real-time, ensuring that the system maintains accurate and up-to-date information throughout the election process, thereby preventing fraud and ensuring the transparency of the voting procedure.

II. OVERVIEW OF EVM

This project presents a novel Electronic Voting Machine (EVM) integrated with Aadhaar-based identity verification and fingerprint biometric scanning, aimed at enhancing the security, integrity, and accuracy of the voting process. By combining Aadhaar data and biometric authentication, the system prevents voter impersonation, multiple voting, and other common fraudulent activities in traditional electoral systems.

One of the most impactful applications of HAR is in healthcare. HAR systems can be utilized to monitor the daily activities of patients, particularly the elderly or those with chronic conditions. For example, fall detection systems can alert caregivers if an individual falls, facilitating prompt assistance. Additionally, HAR can track rehabilitation progress, ensuring patients adhere to prescribed exercise routines.

The EVM operates in two distinct phases: the registration phase, where eligible voters' Aadhaar numbers and fingerprints are securely recorded and verified, and the voting phase, where voters authenticate themselves using the same data before casting their vote. This two-factor authentication ensures that only legitimate voters can participate in the election, and once a voter has cast their vote, they are marked as having voted, preventing multiple voting attempts.

The primary application of this system is in **electoral voting**, where it can be used for **national, regional, and local elections** to enhance security and ensure fair voting practices.

The Aadhaar and fingerprint-based authentication system can be adapted for **secure access control** in high-security areas such as government offices, financial institutions, and research facilities, ensuring that only authorized individuals can enter.

This system can be implemented in **ATMs**, **banking applications**, and **online transactions**, where biometric authentication can serve as a fraud-proof alternative to passwords, making financial transactions more secure.

The technology can be applied to patient identification systems, where biometric verification ensures **accurate patient identification**, reducing the risk of medical errors and improving the management of medical records.

The **fingerprint-based authentication** can be employed in **educational institutions, workplaces**, and **events** to track attendance securely and efficiently, preventing unauthorized access and ensuring accurate records.

This project not only addresses key issues in electoral security but also opens up a wide range of applications for secure identity verification and authentication in various domains. The system's flexibility and scalability make it an innovative solution for both governmental and private sector use, advancing the integration of biometric technology in real-world applications.

III. TECHNOLOGIES AND METHODOLOGIES OF EVM

The proposed Electronic Voting Machine (EVM) with Aadhaar-based verification and fingerprint scanning operates through two main phases: the **Registration Phase** and the **Voting Phase.** Each phase plays a distinct role in ensuring secure, accurate, and fraud-proof elections. Here is an in-depth explanation of each phase:

1. Registration Phase

The **Registration Phase** occurs prior to election day and is essential for building a verified database of eligible voters. During this phase, the following steps are undertaken:

Data Collection:

- Eligible voters must provide their Aadhaar number, a unique 12-digit identification number, to confirm their identity. The Aadhaar number ensures that each voter is unique and minimizes the risk of voter impersonation.

- Voters also provide a fingerprint scan, which is then digitized and stored in the system. Fingerprint biometrics are highly secure, as they capture the unique patterns on each individual's finger, making it almost impossible for someone to duplicate.

Verification and Database Storage:

- The Aadhaar number and fingerprint scan are cross-verified to ensure data accuracy and consistency. This process confirms the eligibility of each voter.
- Once verified, the Aadhaar number and fingerprint data are encrypted and stored in a secure database, linked together to create a unique identity record for each voter. The database is designed to prevent tampering and unauthorized access, ensuring that only legitimate voter data is stored.
- The verification process involves confirming a voter's identity using secure biometric and/or demographic data. In this system, verification typically includes **fingerprint scanning** and, optionally, another unique identifier (e.g., Aadhaar number or a user ID).

Assignment of Voter Status:

- Each registered voter is flagged as **eligible to vote**. This status can only be changed after the voter has successfully cast a vote during the Voting Phase, preventing multiple voting attempts by the same individual.

2. Voting Phase

The **Voting Phase** takes place on election day and utilizes the data collected during the Registration Phase to verify each voter's identity before they are allowed to vote. This phase consists of the following steps:

Aadhaar Number Entry:

- Upon arriving at the polling station, the voter is prompted to enter their Aadhaar number on the EVM. The system uses this number to locate the voter's record in the database.
- If the Aadhaar number is valid and exists in the database, the system proceeds to the next step. If the number is invalid or not registered, access is denied, preventing unauthorized voting.

Fingerprint Authentication:

- Next, the voter places their finger on the fingerprint scanner. The system compares the live scan with the stored fingerprint data associated with the provided Aadhaar number.
- Only if the live fingerprint matches the stored data does the system authorize the voter to cast their vote. This dual authentication (Aadhaar and fingerprint) ensures that only registered and verified voters can participate, eliminating risks of impersonation and fraud.

Vote Casting:

- Upon successful verification, the voter is granted access to the voting interface. Here, they can select their candidate or choice on the EVM screen.
- Once the vote is cast, the system marks the voter's status as voted in the database. This update is crucial to prevent multiple voting attempts, as the system will deny any further voting attempts by the same individual.

Duplicate Voting Prevention:

- If a voter tries to re-enter their Aadhaar number and fingerprint after having already voted, the system will detect the "already voted" status and deny access. This mechanism serves as a security measure to uphold the principle of one person, one vote.

Used technologies

In **fingerprint recognition** systems, two key techniques used to match a **live fingerprint** with a **stored fingerprint template** are **minutiae-based matching** and **pattern matching**. Both are essential for ensuring accurate and reliable biometric verification. Here's an explanation of each method:

Minutiae-based matching:

- Minutiae-based matching focuses on identifying and comparing distinct, unique points within a fingerprint, known as minutiae. These include ridge endings, where a ridge abruptly terminates, bifurcations, where a ridge splits into two, and other features like ridge dots or enclosures. The technique works by extracting these minutiae points from a fingerprint, creating a template that records their position, direction, and type.

- During the matching process, the system compares the minutiae of a live fingerprint to a stored template, evaluating the spatial relationship between them. This method offers high accuracy and is less affected by changes in fingerprint orientation, as it relies on unique, identifiable points. However, it can be sensitive to fingerprint quality, and the matching process can be computationally intensive, requiring precise alignment of minutiae points.

Pattern matching:

- Pattern matching in fingerprint recognition involves comparing the overall ridge patterns of a fingerprint, rather than focusing on individual minutiae points. The primary goal is to analyze the global structure of the fingerprint, such as loops, whorls, and arches.
- These ridge patterns are extracted and analyzed using various algorithms that capture the flow and shape of the ridges. During the matching process, the system compares the live fingerprint's ridge pattern with the stored template by evaluating the similarity of their overall structures.
- Pattern matching is typically faster than minutiae-based matching because it focuses on broader features. However, it is less accurate on its own since similar ridge patterns, such as loops or whorls, may appear in different individuals. Despite this, it can still be useful in cases where minutiae-based methods struggle due to poor fingerprint quality or distortion.

Database Management System:

- The system stores each voter's Aadhaar number, fingerprint data, and voting status in a secure, encrypted database. The database is designed to ensure data integrity and prevent unauthorized access.

Secure Communication and Data Transmission:

- Data transmission between the EVM system and the Aadhaar database is secured using SSL/TLS encryption to ensure that the voter's personal information is securely transmitted.
- Use: Encryption ensures that sensitive data such as Aadhaar numbers and fingerprint data cannot be intercepted or tampered with during transmission.

Real-Time Processing:

- Voter authentication and voting status updates are processed in real-time to ensure that all records are accurate and current. This ensures that once a voter casts their vote, their voting status is immediately updated in the database to prevent multiple voting attempts.
- Use: Real-time updates allow the system to check the voter's status, validate their credentials, and update their record as "voted" upon successful voting.

Secure Fingerprint Scanner:

- The fingerprint scanner uses optical or capacitive technologies to capture the fingerprint image and extract biometric features. The image is processed using feature extraction algorithms to identify key points, which are then compared with the stored fingerprint data.
- Use: The fingerprint scanner plays a critical role in biometric authentication, ensuring accurate identification by verifying the physical characteristics of the voter's fingerprint.
- The **minutiae-based method** analyzes specific fingerprint details and compares them to a stored template, providing accurate and reliable matching with minimal error.
- Advanced scanners integrate anti-spoofing measures, such as **liveness detection**, which can detect real, live fingerprints versus replicas or photos.

IV. WORKING

The **Arduino Uno** is the central controller of the Electronic Voting Machine (EVM) system, connecting to various components such as the **fingerprint scanner**, **Aadhaar card reader** (or keypad for manual input), and **16x2 LCD display**. The fingerprint scanner sends biometric data to the Arduino, which compares it to the stored template for verification. The Aadhaar card reader or keypad allows the voter to input their Aadhaar number, which is then verified against the database via a **Wi-Fi module** (ESP8266) or a direct serial connection. The LCD display communicates real-time information to the voter, such as prompts or error messages, while the Arduino manages the data flow and updates the database with the voter's status after casting their vote. Power is supplied to all components to ensure smooth functioning throughout the voting process.

V. CONCLUSION

In summary, the Electronic Voting Machine (EVM) system proposed in this project, integrating Aadhaar-based verification and fingerprint scanning, represents a significant advancement in electoral technology. By utilizing the unique identifiers provided by Aadhaar and the biometric fingerprint authentication, this system ensures a higher level of voter security, preventing fraudulent activities such as multiple voting attempts and identity theft. The use of the minutiae-based matching algorithm for fingerprint verification plays a crucial role in accurately identifying the voter by comparing their live fingerprint with the stored template, enhancing the authenticity of the process. The algorithm's efficiency in matching minutiae points ensures that only valid voters are permitted to cast their vote. Additionally, the Aadhaar number verification adds an extra layer of security, ensuring that each individual is correctly identified and registered. Overall, the system offers a reliable, secure, and transparent voting process, addressing the limitations of traditional EVMs and paving the way for a more efficient, fraud-resistant election system.

VI. REFERENCES

[1] Unique Identification Authority of India (UIDAI). "Aadhaar Authentication System Overview." UIDAI, Government of India.https://uidai.gov.in

[2] Jain, Anil K., et al. "Fingerprint Matching Using Minutiae and Ridge Patterns." IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 8, 1997, pp. 844-857. DOI: 10.1109/34.618248

[3] Maltoni, Davide, et al. "Handbook of Fingerprint Recognition." Springer Science & Business Media, 2009. ISBN: 978-0-387-77685-2

[4] Banzi, Massimo. Getting Started with Arduino. 2nd Edition, O'Reilly Media, 2011. ISBN: 978-1-4493-9471-2.

[5] Ratha, Nalini K., et al. "Minutiae Based Fingerprint Matching." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 1996.
https://ieeexplore.ieee.org/document/557249 2014,

[6] Garcia-Molina, Hector, and Kenneth P. Birman. "Security Issues in Electronic Voting Systems." IEEE Computer Society, 2003. DOI: 10.1109/ICDCS.2003.1203594

[7] Maltoni, Davide, et al. "Fingerprint Recognition: A Survey." Proceedings of the IEEE, vol. 85, no. 9, 1997, pp. 1408-1424.