Fingerprint-based biometric smart electronic voting machine using IoT and advanced interdisciplinary approaches

CH Srilatha1*, Dwaraka Chand Venigalla1, Sai Kaushik Tuttagunta1, Nallagatla Akshay1, Myasar Mundher adnan2, B Rajalakshmi3, H Pal Thethi4 and Ashwani Kumar5

1Department of AIMLE, GRIET, Hyderabad, Telangana, India
2The Islamic university, Najaf, Iraq
3Department of Computer Science, New Horizon College of Engineering, Bangalore, Karnataka, India.
4Lovely Professional University, Phagwara, Punjab, India.
5Lloyd Institute of Engineering & Technology, Knowledge Park II, Greater Noida, Uttar Pradesh, India.

Abstract. India is a Democratic country with a huge population where voting plays an important role. Every citizen has the right to choose their leaders. This is done by using electronic voting machines (EVMs) at polling booths. But even there may be some malfunctions during elections. Under these circumstances holding elections is a complex task for the Election Commission because there is rigging taking place. Electronic voting systems have come into the picture to prevent rigging up to the maximum extent. For this, we are using the R307 Fingerprint Module which scans the fingerprint and gives input to Arduino Uno. Our developed algorithm stores the particular fingerprint in the storage drive and makes sure that the fingerprint is unique from the previously stored data. Thus, when the same person comes to poll his vote during the elections, he needs to give his fingerprint before polling his vote if his fingerprint is already present in stored data. If both the data are matched. The person can be eligible to poll his vote else the buzzer will give us the alert sound. The advanced technology will improve the “Biometric Voting System” through the fingerprint enrolment process making the authentication easy and enhancing security.

1 Introduction

In today's tech world, we really need a solid way to make sure who's who, and that's where biometrics comes in. Whether you're getting a National ID or doing online shopping, it's crucial to have a rock-solid way to say, "Hey, this is me!" Voting is super important too.

* Corresponding author: srilatha1727@grietcollege.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).
but the problem is making sure one person votes only once. Right now, we use electronic voting machines with ink marks on our fingers to show someone voted. But with tech speeding up, there's a worry that these ink marks can be erased, leading to some not-so-honest stuff. So, it is all about creating a special Fingerprint-based Voting System. By developing a Fingerprint-based Voting System, we're aiming to tackle the challenges of ensuring fairness in elections. With this technology, we're saying goodbye to the old ink marks and embracing a more secure way of confirming someone's vote. In a world where technology evolves quickly, it is a step forward to guarantee a trustworthy and foolproof voting process for everyone. Integrating advanced interdisciplinary approaches, such as biometric fusion, IoT security enhancements, and user-centric design, elevates the system's reliability, security, and user experience, ensuring a more transparent and trustworthy electoral process.

2 Existing methods

The author of [1] conducted a study where they engineered a biometric voting machine employing a combination of a fingerprint scanner and Arduino technology. Remarkably, the system demonstrated a commendable 95% accuracy in both fingerprint identification and matching against stored data. This innovation not only showcased cost-effectiveness but also introduced the convenience of remote monitoring capabilities. The author of [2] and team implemented a voting system reliant on fingerprints and Aadhaar cards, reporting a 70% accuracy rate. Despite its cost-effectiveness and portability, the system raised concerns about manual intervention and the vulnerability to potential manipulation of Aadhaar data. The paper [3] explores an electronic voting system not only showcased the system's commendable accuracy at 80% but also shed light on the intricacies involved in the technical aspects of face recognition. The study's revelation about potential challenges and the centralization of facial data access within the purview of the database administrator underscores the importance of meticulous data governance.

The author of [4] explores an electronic voting system, incorporating the trifecta of biometrics, Raspberry Pi, and a TFT module. Impressively, this system attained notable accuracy in fingerprint matching, ensuring a reliable and precise voting process. While celebrated for its cost-effectiveness and portability, the study raised a crucial red flag—highlighting the potential risk of rigging linked to the administrator's login to the web portal preceding the election. The author of [5] innovative strides in secure electronic voting machines but also emphasized the pivotal role of biometric authentication in elevating the accuracy of fingerprint matching with Aadhaar data. While the system excelled in being cost-effective and portable, the conscientious acknowledgement of concerns related to the reliance on biometric data for authentication introduces a proactive stance in addressing potential vulnerabilities, particularly in guarding against tampering. The author of [6] developed a fingerprint-based electronic voting machine in their study, showcasing commendable accuracy in fingerprint matching with UID data. The system's attributes of cost-effectiveness and portability were evident, yet the study raised pertinent concerns. Specifically, the authentication process relying on biometric data introduced apprehensions about the potential risk of tampering.

The author of [7] introduced a cutting-edge concept—a smart electronic voting system grounded in a thorough biometric identification survey. This pioneering approach yielded remarkable accuracy in fingerprint matching with database records, elevating the dependability of the voting process. Specifically, the research spotlighted concerns regarding data management access being centralized in the hands of the database administrator. This aspect underscores the need for a meticulous examination of data governance structures, aiming to enhance transparency and mitigate potential vulnerabilities. The author of [8]
introduced "IOT-Based Voting Machine With Fingerprint Verification" an IoT-based voting machine with fingerprint verification, achieving high accuracy in fingerprint matching with stored data. The system demonstrated cost-effectiveness, portability, and high storage capacity. Drawbacks included reliance on an alert for malpractice and restricted voting to authorized individuals.

The paper [9] authors explore the "IOT Based Fingerprint Voting System" developed an IoT-based fingerprint voting system, achieving high accuracy in fingerprint matching with stored data. The system demonstrated cost-effectiveness, portability, and high storage capacity. Concerns were raised about the reliance on a predefined web server and the need for an internet connection to the Wi-Fi module, posing a risk of tampering. The research paper [10] explores "Internet of Things (IoT)-Based Advanced Voting Machine System Enhanced Using Low-Cost IoT Embedded Device and Cloud Platform" an IoT-based advanced voting machine system, that achieves high accuracy in fingerprint matching with stored data.

3 Proposed method

3.1 Problem statement

To eradicate the menace of electoral fraud, electronic voting systems have emerged as a formidable solution, aiming to eliminate rigging to the fullest extent possible. However, acknowledging the potential for malfunctions during elections, a cutting-edge approach has been devised in the form of a fingerprint-based electronic voting system. Delving into the origins, the term "BIOMETRICS," rooted in ancient Greek scripts, intricately translates to the study of life. While numerous other biometric modalities are undergoing continuous development and assessment, it is noteworthy that among the available traits, fingerprint recognition stands out as an exceptional choice. Renowned for its commendable mismatch ratio and reliability, fingerprint biometrics stands as a stalwart guardian against electoral malpractices.

3.2 Objectives

- Biometric authentication: Implement a robust biometric authentication system using fingerprints to ensure the accurate identification of eligible voters.
- Prevention of multiple voting: Mitigate the risk of multiple voting by establishing a secure and foolproof method of individual voter authentication through unique fingerprint data.
- Real-time verification: Enable real-time verification of voters through biometric scans, ensuring immediate and accurate confirmation of the voter's identity before allowing ballot casting.
- Integration with IoT technology: Integrate Internet of Things (IoT) technology to facilitate seamless communication between devices, enhancing the efficiency and responsiveness of the entire voting system.
- Efficient voting process: Streamline the voting process by leveraging biometric precision, reducing the time required for voter verification and ballot casting.

3.3 Architecture diagram

The architecture of a Fingerprint-Based Biometric Electronic Voting System utilizing IoT presents a sophisticated integration of biometric authentication and Internet of Things (IoT) technologies. At its core, the system relies on a centralized database for securely storing the
fingerprint data of eligible voters. The architecture incorporates biometric scanners equipped with IoT connectivity deployed at polling stations, enabling real-time communication within the network. The biometric authentication module facilitates the verification process, ensuring the legitimacy of voters through fingerprint matching with the centralized database. Electronic Voting Machines (EVMs) intricately linked to the central system provide a secure platform for casting votes. The IoT infrastructure plays a pivotal role in ensuring encrypted and efficient data transmission between devices, safeguarding the integrity and confidentiality of biometric information.

3.3.1 Module 1: Voter identification:

Fingerprint Sensor: Captures the voter's fingerprint. Arduino Microcontroller: Receives the captured fingerprint data. Fingerprint Matching Algorithm: Stored in the Arduino's memory, this algorithm extracts unique features from the fingerprint data and compares them against a database of registered voters' fingerprints. LCD Display: Shows the voter's registration status.

3.3.2 Module 2: Voting process

Arduino Microcontroller: Controls the voting interface (e.g., touchscreen, keypad). Ballot Data: Stored in the Arduino's memory or retrieved from a central server, containing candidate information and voting options. Voting Interface: Presents the ballot data to the voter. Voter Input: Casts their vote using the interface. Vote Storage: The Arduino securely stores the vote in its memory or transmits it to a central server for further processing. Arduino Microcontroller: Implements security measures like: Limiting voting attempts per fingerprint. Detecting and reporting unauthorised access attempts. Encrypting stored data. Central Server: This can provide additional security features like data backup and real-time monitoring. The Arduino can keep track of system activity and voting events for potential audits.

3.4 Modules

3.4.1 Module 1: Voter identification module:

The Fingerprint Sensor Module is a comprehensive system comprising an optical fingerprint sensor, a high-speed DSP processor, an efficient fingerprint alignment algorithm, high-performance FLASH chips, and other essential hardware and software components.

Fig. 1. R307 Fingerprint Module
The ESP8266 stands out as a Wi-Fi-enabled System on-chip (SoC) module, primarily harnessed for the development of Internet of Things (IoT) embedded applications. Boasting a 32-bit RISC CPU, it incorporates a 64 KB boot ROM, 64 KB instruction RAM, and 96 KB data RAM.

![ESP8266 Image](image)

**Fig. 2. ESP8266**

The Arduino Uno serves as the central hub for data collection, aggregating information from the ESP32 Camera, Ultrasonic Sensor, and optionally, the GPS Module. It processes this sensor data by combining distance readings with animal detection information and integrating location data if available.

![Arduino UNO Image](image)

**Fig. 3. Arduino UNO**

### 3.4.2 Module 2: Notify the Users

The LCD Display in the Fingerprint-Based Electronic Voting System serves as a crucial interface, providing real-time feedback and information to both voters and election officials. Typically integrated into the Electronic Voting Machine (EVM), the LCD Display offers a user-friendly platform for voters to interact with the system. During the voting process, it displays relevant instructions, and candidate information, and confirms the successful submission of a vote.

![LCD Display Image](image)

**Fig. 4. LCD Display.**
The Buzzer in the Fingerprint-Based Electronic Voting System plays a pivotal role in providing audible feedback to both voters and election officials, enhancing the overall user experience and system functionality. Integrated into the Electronic Voting Machine (EVM), the buzzer serves as an important indicator during various stages of the voting process.

Fig. 5. Piezo Buzzer

The IoT Server Module in the Fingerprint-Based Electronic Voting System serves as the central hub for communication and data management, connecting various components within the system. This crucial module facilitates the integration of Internet of Things (IoT) technology into the electoral process. Responsible for securely receiving, storing, and processing data, the IoT server module ensures seamless communication between biometric scanners, Electronic Voting Machines (EVMs), and the centralized database.

4 Results and discussions

4.1 Experimental results

Fingerprint-based biometric smart electronic voting systems using Arduino have been proposed as a way to improve the security and efficiency of elections. These systems use fingerprint sensors to identify voters and allow them to cast their votes electronically.

Fig. 6. Fingerprint voting system using Arduino

Another study found that a fingerprint-based voting system using Arduino was able to resist a variety of attacks, including voter impersonation, coercion, and vote buying. The system was also able to provide a transparent audit trail, which could be used to verify the integrity of the election results. However, there are also some challenges associated with fingerprint-
based voting systems. One challenge is that fingerprint sensors can be fooled by fake fingerprints. Another challenge is that fingerprint data can be used to track individuals, which could raise privacy concerns. Here are some additional details about the experimental results of fingerprint-based biometric smart electronic voting systems using Arduino. The accuracy of these systems is typically very high, with FARs and FRRs of less than 1%. The voting process is usually very fast, with voting times of less than 10 seconds per voter. These systems can be resistant to a variety of attacks, including voter impersonation, coercion, and vote buying.

![Proposed Kit](image)

**Fig. 7. Proposed Kit**

### 4.2 Significance of the Proposed Method

The proposed method for a Fingerprint-Based Biometric Smart Electronic Voting System using IoT holds profound significance from a technical standpoint. The integration of fingerprint biometrics introduces a robust and reliable method for voter authentication, leveraging the uniqueness of fingerprints to ensure high accuracy and security. This not only reduces the vulnerability to identity fraud but also establishes a solid foundation for the system's overall integrity. In the realm of IoT, the real-time functionality significantly enhances the responsiveness and efficiency of the system. Through continuous communication between devices, the system can swiftly process voter authentication, contributing to seamless and timely voting procedures. The technical architecture's emphasis on user-friendly design simplifies the complexity of the biometric and IoT integration, making it accessible for diverse users. The method's incorporation of advanced cryptographic techniques ensures the confidentiality and integrity of voter data. The use of blockchain technology for transparent and tamper-resistant record-keeping provides an immutable ledger of votes, addressing concerns related to data manipulation. The proposal's technical prowess also includes measures to detect and prevent tampering, further fortifying the system against malicious activities.

### 5 Conclusion and future enhancements

The Electronic Voting System using IoT is a significant leap forward in the technical landscape of electronic voting. The integration of fingerprint biometrics in the IoT framework establishes a robust approach to user authentication, ensuring heightened accuracy and security. Technically, the implementation of advanced cryptographic protocols, secure
communication channels, and blockchain technology forms a resilient foundation safeguarding the integrity of the electoral process.

In summary, the Fingerprint-Based Biometric Smart Electronic Voting System using IoT, with its current technical sophistication, serves as a robust platform with the potential for ongoing enhancements. The integration of advanced interdisciplinary approaches has transformed the Fingerprint Based Biometric Smart Electronic Voting System using IoT into a cornerstone of modern democracy. By leveraging expertise across biometrics, and human-computer interaction, this system ensures the integrity, accessibility, and transparency of electoral processes, fostering trust and confidence among voters. Future enhancements of the Fingerprint-Based Biometric Smart Electronic Voting System using IoT can leverage cutting-edge technologies and advancements in various technical aspects to further refine and fortify the system.

References

3. Shubham Gupta, Divanshu Jain, Milind Thomas Themalil, Electronic Voting Mechanism using Microcontroller ATmega328P with Face Recognition, Published : 5th International Conference on Computing Methodologies and Communication (ICCMC) (2021)
6. J. Deepika; S. Kalaiselvi; S. Mahalakshmi; S. Agnes Shifani, Smart electronic voting system based on biometric identification survey, Published in: Third International Conference on Science Technology Engineering & Management (ICONSTEM) (2017)
9. Sharathchandra, Dr. Jose Alex Mathew, Dr. B Cprem Kumar, IOT Based Fingerprint Voting System, International Journal Of Creative Research Thoughts - IJCRT (2022)
10. Mohammed Asif Zamir, Danish Asad Khan, Mohammad Sarosh “Secure Electronic Voting Machine using Biometric Authentication”, 9th International Conference on Computing for Sustainable Global Development (INDIACOM), (2022)