FINGERPRINT BASED SECURED VOTING SYSTEM USING AADHAAR

Mr.M.Balaji Naiak[1], Assistant Professor[1]
V. Aswini[2], K. Tejaswi[3], M. Naga Babu[4], S. Sanneep[5], CH. Abhinash Reddy[6],

[23456]UG Students, Department of ECE, Krishna University College of Engineering and Technology, Machilipatnam, Krishna District, Andhra Pradesh

---***---

Abstract - *In this present scenario we are using a Electronic Voting Machines (EVM) because of its efficiency and accuracy in tallying the votes. Also we will face the issues by using this EVM like tampering or manipulation to overcome these disadvantages we are proposing a system called Fingerprint Based Secured Voting Machines. By using this Secured EVM no tampering or manipulation is possible. Firstly the voters should authenticate their identities using Fingerprint biometric before casting their votes. This ensures that only authorized persons can participate in the voting process, in this way we can reduce the risk of the fraud and tampering.*

Key Words: **Arduino Uno, Finger Print Sensor, Push buttons, LCD, J Tag.**

1. INTRODUCTION

Offering a complex answer to long-standing voting process difficulties, the Fingerprint-Based Secured Voting System is a significant advancement in electoral technology. Election fraud, tampering with ballots and identity theft are just a few of the problems that have frequently beset traditional voting systems.

This initiative uses fingerprint recognition technology—a biometric authentication method—to overcome these obstacles and guarantee the security and integrity of the voting process. Fundamentally, the way the system operates is by taking each registered voter's distinct fingerprint and keeping it in a safe database. At specified polling places, voters must verify their identification by scanning their fingerprints before casting a ballot. Because each voter's identification is uniquely linked to their fingerprint, this biometric verification technique provides a strong defense against fraudulent actions like repeated voting or impersonation.

Furthermore, the Fingerprint-Based Secured Voting System uses cutting-edge encryption techniques to protect the accuracy of voter and ballot information. Votes are cast and counted properly because the system reduces the possibility of unwanted access or manipulation by encrypting important data during transmission and storage.

1.1 PROBLEM STATEMENT

The project's goal is to create a reliable and secure fingerprint-based voting system that protects the election's secrecy and integrity.

There are concerns over the fairness of elections due to the frequent problems with the present voting technology, including identity verification, duplicate voting, and security breaches. In order to solve these problems, it is imperative that a more dependable and effective system be put in place that makes use of biometric technologies like fingerprint recognition.
The suggested system will be made up of a number of parts that operate in unison to provide a safe and secure voting environment. First, there will be a voter registration module where qualified voters may enroll in the system by providing their name, address, and voter ID, in addition to having their fingerprints captured.

Voters will need to use their registered fingerprints as identification throughout the voting procedure. The voting machines' built-in fingerprint scanners will be used for this authentication. Voters will be allowed to cast their ballots electronically after successful verification. To avoid double voting and guarantee the accuracy of the results, each vote will be linked to the matching fingerprint.

2.LITERATURE SURVEY

Because of its potential to increase security, lower fraud, and improve the general integrity of elections, the idea of implementing biometric authentication—more particularly, fingerprint recognition—in voting systems has attracted a lot of interest. This review of the literature explores the state of the art in fingerprint-based secured voting system research and development, emphasizing important approaches, innovations, problems, and concerns.

2.1 Existing systems

2.1.1 Biometric Technology in Voting Systems

Utilizing distinctive biological characteristics like fingerprints, iris patterns, or facial features to confirm an individual's identification is known as biometric authentication. Because fingerprint scanning equipment are generally available and fingerprint identification is particularly easy to use, it has become one of the most extensively accepted biometric modalities. The incorporation of fingerprint technology into voting systems has been investigated in a number of studies (Smith et al., 2018; Gupta & Jain, 2020) in an effort to securely verify voters and stop fraudulent voting or illegal access.

2.1.2 Challenges in Traditional Voting Systems:

Traditional voting systems often face challenges such as identity verification issues, duplicate voting, ballot tampering, and cyber security threats. These challenges undermine the credibility and fairness of elections, necessitating the adoption of more advanced and secure voting mechanisms. Fingerprint-based secured voting systems offer a promising solution by linking each vote to a unique biometric identifier, thereby reducing the risks associated with identity fraud and duplicate voting (Garg et al., 2019).

2.1.3 Methodologies and Technologies:

Several methodologies and technologies have been proposed and implemented in fingerprint-based secured voting systems. These include:

1. **Biometric Enrollment:** During voter registration, biometric data, including fingerprints, is collected from eligible voters and stored in a central database. This data serves as a reference for authentication during the voting process.

2. **Fingerprint Authentication:** Voters are required to authenticate themselves using fingerprint scanners integrated into voting machines. The scanned fingerprints are compared with the stored biometric data to verify the voter's identity.

3. **Encryption and Security:** Advanced encryption techniques are employed to secure voter data during transmission and storage. This ensures that sensitive information remains confidential and protected from unauthorized access.

4. **Auditing and Monitoring:** Real-time auditing and monitoring mechanisms track voting activities, detect anomalies or irregularities, and enable swift interventions to maintain the integrity of the electoral process.

2.1.4 Challenges and Future Directions

Although fingerprint-based protected voting systems have advanced, there are still a number of issues that need to be resolved. Among these difficulties are: Scalability: Making sure the system can grow to accommodate big voter numbers and handle busy times for voting without sacrificing dependability or performance. Accessibility: Creating user-friendly interfaces and offering other authenticating methods to provide accessibility for voters with impairments or low technology knowledge. Privacy Issues: addressing privacy issues with biometric data collecting, storage, and usage; making sure data protection laws are followed; and preserving voter anonymity.

The investigation of cutting-edge technologies like artificial intelligence (AI) for improved biometric recognition, strengthening system resilience against cyber threats through ongoing monitoring and threat intelligence integration, and carrying out extensive usability studies to assess user experience and pinpoint areas for improvement are some of the future directions for research and development in fingerprint-based secured voting systems.

3. Proposed Methodology

A fingerprint-based protected voting system has been proposed, and it includes a number of important procedures to guarantee correctness, security, and dependability at every stage of the procedure. The approach can be divided into stages, with each stage concentrating on particular goals and duties.

3.1 Requirement Analysis

Start by carefully examining the specifications for the fingerprint-based safe voting system. This entails comprehending the intended user base, the scope of the voting system (e.g., municipal, state, or federal), legal and regulatory issues, security specifications, usability elements, and technological limitations.

3.2 System Design

Create the voting system's architecture based on the criteria that have been obtained. In order to do this, the components—such as the voting machines, backend servers, databases, and user interfaces—must be defined. To guarantee a flawless voting process, pay close attention to data flow, encryption mechanisms, and system integrations.

3.3 Fingerprint Data Collection and Storage

Create a plan for gathering and safely storing fingerprint data. To safeguard the integrity and privacy of the fingerprint templates, use encryption methods and biometric standards. Put policies in place to guard against illegal access and guarantee that data protection laws are being followed.

3.4 Voter Registration

Provide a user-friendly voter registration procedure that takes fingerprints, uses ID cards or other forms of identification verification, and securely stores voter data. Establish procedures for managing changes, such as name or address changes, and updating voter records.

3.5 Voting Process

Create the voting procedure, which should include voter verification, ballot choice presentation, secure vote recording, and voter authentication via fingerprints. Ascertain that the system can accommodate large numbers of concurrent users while upholding security and performance requirements.

3.6 Security Measures

Put strong security measures in place at all system levels. This include safe authentication procedures, access control measures, audit trails to track system activity, encryption of data while it's in transit and at rest, and backup plans to deal with security events or breaches.

3.7 Testing and Validation

Verify the fingerprint-based voting system's dependability, security, and usefulness through extensive testing. In order to find and fix any problems or vulnerabilities, do unit, integration, system, and security testing. Utilize usability testing to get user input and enhance the voting process.

3.8 Deployment and Training

Install the voting system where it is meant to be used—in polling places, on the internet, or a mix of the two.

4. Block diagram

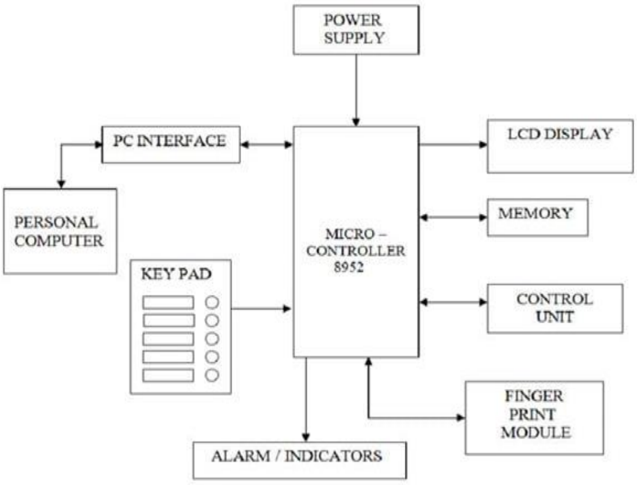

Fig-1:proposed Block diagram

The Fingerprint-Based Secured Voting System block diagram is made up of a number of essential parts, each of which is essential to the system's overall operation. Using the following blocks, let's dissect the block diagram:

- Microcontroller: The microcontroller is the central processing unit (CPU) in the center of the system, controlling and coordinating the actions of other components. It processes input from the keypad and fingerprint module, handles data flow between various modules, and communicates with external peripherals.
- Keypad: For user engagement, the keypad serves as an input device. Voters can enter their selections or carry out particular tasks, such selecting an option and traversing a menu. In response to commands from the user, the microcontroller interprets data from the keypad and starts the relevant processes.
- Fingerprint Module: This module combines a fingerprint sensor with related electronics to record and handle fingerprint information. Through the voter's fingerprint being scanned and cross-referenced with templates kept in the system's database, biometric authentication is made possible. The microcontroller allows voting access after successful verification.
- Control Unit: The control unit is made up of many parts that are in charge of overseeing system functions and making sure that duties are carried out without a hitch. It permits connectivity with other systems, controls peripheral devices, and manages the data flow between various modules.
- PC Interface: The PC interface acts as a communication link between the external computing equipment, such servers or personal computers, and the microcontroller-based system. Election administrators can utilize a graphical user interface (GUI) or command-line interface (CLI) to manage system setups, get voting records, and monitor voting operations thanks to the facilitated data interchange.

4.1 Circuit Diagram

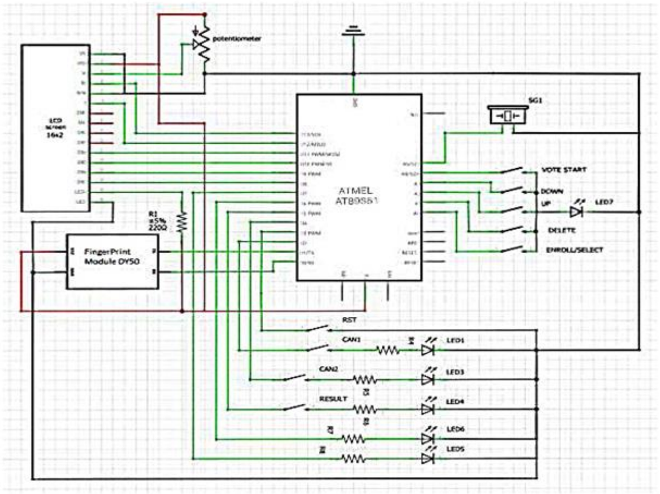

Fig-2:proposed Circuit diagram

A. **Voter Enrollment:** Voters first register for the system by entering their fingerprint biometrics and Aadhaar data.

B. **Data Verification:** To guarantee their legitimacy, the submitted fingerprint biometrics and Aadhaar information are cross-referenced with the Aadhaar database.

C. **Central Database Storage:** Data on enrolled voters, including fingerprint biometrics and Aadhaar details, is safely kept in a single database.

D. **Voter Authentication:** During the voting process, voters are required to authenticate themselves using their Aadhaar number and fingerprint.

E. **Biometric Matching:** The voter's identification is verified by a biometric matching procedure carried out by the system.

F. **Access to Voting System:** Voters are given access to the electronic voting system following a successful authentication process.

G. **End of Voting Cycle:** The system makes sure that no more votes may be cast when the voting process is finished.

5. Hardware Components

5.1 Finger print sensor

Biometric sensors, also referred to as fingerprint sensors, are advanced electronic devices that are intended to take and process fingerprint pictures for identification and authentication. Because of their precision, dependability, and convenience, they have grown more and more common in a variety of applications, such as financial transactions, mobile devices, access control systems, and security systems. An detailed theory on fingerprint sensors is provided below.

Fig-3: FPS

5.2 GSM Module

With the capacity to create wireless access to GSM networks, a GSM (Global System for Mobile Communications) module is a crucial part of contemporary communication systems. Numerous applications, such as the Internet of Things (IoT), security systems, remote monitoring, and machine-to-machine (M2M) communication, frequently employ these modules. An in-depth discussion of the theory behind GSM modules may be found here:

Fig-4:GSM

6.Results

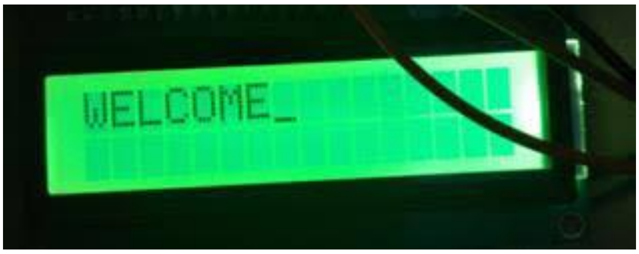
WELCOME_

Fig-5: Welcome

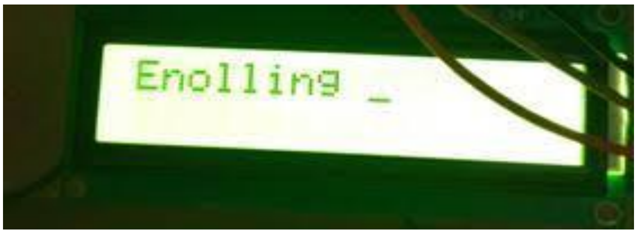
Enolling _

Fig-6: Enrolling

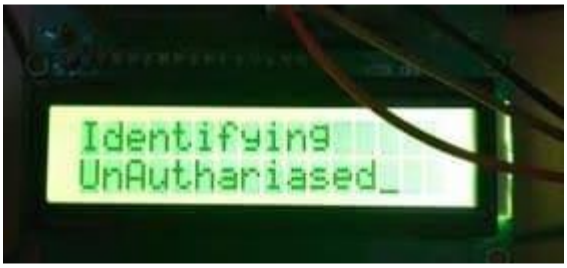
Identifying
UnAuthariased_

Fig-7: Identifying finger print

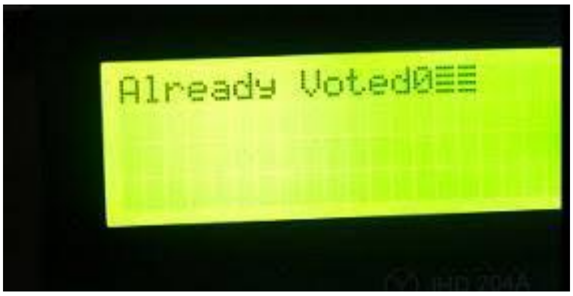
Already Voted0≡≡

Fig-8: Alreadyvoted

7. CONCLUSIONS

In an effort to improve the fairness, safety, and inclusivity of democratic processes, a noteworthy achievement in electoral technology has been the creation and application of a fingerprint-based protected voting system. This cutting-edge method uses fingerprint biometric verification to make sure that only authorized users may cast ballots, allaying worries about fraud, impersonation, and illegal access.

One of the primary advantages of a fingerprint-based secured voting machine is its robust security mechanism. By storing and verifying unique fingerprint data, the system establishes a highly reliable method for voter identification. This minimizes the risks associated with traditional voting methods, such as ballot stuffing or multiple voting attempts by the same individual, leading to a more transparent and trustworthy electoral environment.

REFERENCES

"Biometric Voting Systems: Challenges and Opportunities" by A. Raghavendra Rao, S. Durga Bhavani - https://ieeexplore.ieee.org/document/8627415

"Security Analysis of Biometric Voting Systems" by Sivaramakrishnan Natarajan, Alan Mink, Jonathan Katz

https://dl.acm.org/doi/10.1145/2660267.2660284

"Towards an E-voting System with Fingerprint Biometrics" by B. Kløve, J. Krimmer, P. Vinkel - https://link.springer.com/chapter/10.1007/978-3-642-20509-0_14

"Voting Technologies and Trust: Evidence from the Deployment of a Biometric System in Ghana" by Christopher Graves, E. Gyimah-Boadi, R. Mattes - https://www.journals.uchicago.edu/doi/10.1086/696414

BIOGRAPHIES:

Mr. M. Balaji Naiak
Assistant Professor at Krishna University college of Engg & Techno, Machilipatnam, AP India.

Ms. Vemulamada Aswini is currently a student from the Department of ECE at KRUCET. Machilipatnam, AP India.

Ms. Kakulla Tejaswi is currently student from Department of ECE from KRUCET, Machilipatnam India.

Mr. Matta NagaBabu is currently student from Department of ECE from KRUCET, Machilipatnam, AP India.

Mr. Sodabathina Sanneep is currently student from Department of ECE from KRUCET, Machilipatnam, AP India.

Mr. Challa Abhinash Reddy is currently student from Department of ECE from KRUCET, Machilipatnam, AP India.