International Journal of Innovative Research in Engineering
Volume 4, Issue 3(May-June 2023), PP: 46-49.
www.theijire.com ***ISSN No: 2582-8746***

RFID Based For Biometric Voting Machine

Maheskumar V[1], Karthikeyan K[2], Chandru P[3], Gunaseelan M[4], Hemanth Kumar Reddy P[5], Vasundharadevi S[6]
[1] *Associate Professor, Department of Computer Science and Engineering, Paavai Engineering College, Namakkal, Tamilnadu, India.*
[2,3,4,5,6] *UG Students, Department of Computer Science and Engineering, Paavai Engineering College, Namakkal, Tamilnadu, India.*

How to cite this paper:
Maheskumar V[1], Karthikeyan K[2], Chandru P[3], Gunaseelan M[4], Hemanth Kumar Reddy P[5], Vasundharadevi S[6]. "RFID Based For Biometric Voting Machine", IJIRE-V4I03-46-49.

https://www.doi.org/10.59256/ijire.2023040353

Abstract: *The Internet of Things (IoT) is a current era that permits digital devices, software, sensors, vehicles, and home appliances to interconnect with networks and transfer data without human or computer intervention. However, the current electronic voting machines lack recent security measures that allow voters to verify their identity before casting their vote, which can lead to false voters casting duplicate or fake votes. To address this issue, a proposed system utilizes RFID and IoT to enhance security mechanisms in electronic voting machines. The system replaces the traditional voter ID with an active RFID tag that the system can scan and match with collected fingerprints. To verify their identity, the voter must scan their RFID tag and confirm their identity with their fingerprints. The voting machine includes an active reading device (reader) to read data on the RFID tag and a fingerprint scanner to capture fingerprints. If the fingerprints match against the database, the individual can cast their vote. In addition, the voting machine includes an LCD display to show the voter's relevant information from the database. This approach can help prevent illegal voting or impersonation since fingerprints are unique to each individual. This paper describes the layout and operation of a Smart Electronic Voting Machine the usage of Arduino UNO, RFID, to improve the election process by preventing electoral fraud and ensuring safety, security, reliability, and seamless conduct of elections in the country. The proposed solution involves the device communicating with the RFID tag. When the voter scans their RFID card, the controller verifies the ID, and if it matches, the LCD displays the result and enables the voter to cast their vote for the corresponding party. It is essential to ensure the secure implementation of the system.*

I.INTRODUCTION

The definition of the Internet of Things (IoT) refers to the community connectivity and computing functionality that extends to objects, sensors, and everyday items, enabling them to generate, exchange, and consume data with minimal human intervention. Although thereis no universal definition, IoT is a technology that enables devices to create A international conversation community with the aid of using replacing records thru the net and appearing on the records. The concept of IoT has been around for two decades, with Kevin Ashton of MIT first using the term in 1999. Since then, various IoT devices have been introduced, including smart televisions, RFID tags within supply chains, and self-driving cars. The IoT accommodates linked clever gadgets that use embedded era to collect, store, and ship records from their surroundings. These devices communicate with each other and act on the information they acquire. With an exponential growth in connected devices, each IoT device communicates packets of data that require reliable connectivity, storage, and security. Managing, monitoring, and securing immense volumes of data and connections from dispersed devices can be a challenge for organizations. However, in a cloud-based environment, this challenge can be effectively addressed. Overall, IoT has made a large effect on the sector in its infancy and could keep growing in significance with inside the future

II.EXISTING SYSTEM

Electronic voting systems have been developed and approved in some developed countries. However, they still face several issues, such as increased costs, a single point offailure, and the possibility that a voter's vote is registered for the wrong candidate. These issues have resulted in instances of rigging and malpractices during the election process. A solution to these issues could be the development of a sophisticated electronic identification system that can identify voters and confirm their authenticity. To address this, a system based on Radio-Frequency Identification (RFID) for voter identification has been proposed. An embedded Microcontroller (LPC2148) ARM7 is used to analyze the data received from the RFID reader. The Microcontroller is provided with a database of all the voters and their voter IDs. After receiving the voter ID from the RFID reader, the Microcontroller compares it with its database to confirm the authenticity of the voter. In conclusion, while electronic voting systems have the potential to streamline the election process, they still face several issues that need to be addressed. The proposed system based on RFID and an embedded Microcontroller could help improve the authenticity of the voting process and reduce instances of rigging and malpractices.

III.PROPOSED SYSTEM AND ARCHITECTURE

Electronic voting systems have been in use for some time now, but they are not without their issues. Concerns includeincreased costs, a single point of failure, and the possibility of a voter's vote being registered for a candidate other than theirchoice. To address these concerns, a finger print-based biometric voting machine using Arduino is being developed. This will ensure thata person can only vote once and that the vote is registered for the voter's preferred candidate. Theproposed system consists of a Control Unit and a Balloting Unit, connected by a five-meter cable. The Control Unit is with the Presiding Officer or a Polling Officer, and the Balloting Unit is positioned in the vote casting compartment. Instead of issuing a poll paper, the Polling Officer will press the Ballot Button at the Control Unit, allowing the voter to cast their vote by pressing the blue button on the Balloting Unit against the candidate and symbol of their choice. The controller used in Electronic Voting Machines (EVMs) has its operating program permanently etched in silicon by the manufacturer, preventing the program from being changed once the controller is manufactured. However, the voter ID checking process in current systems is manual, which could lead to illegal voting by the wrong candidate and the possibility of multiple votes by the same person. To improve the security of the voting machine, RFID is used as a vote ID card in this project. Additionally, human fingerprintis used to cast the vote, making it difficult for anyone to forge a vote since every human's fingerprint is unique.

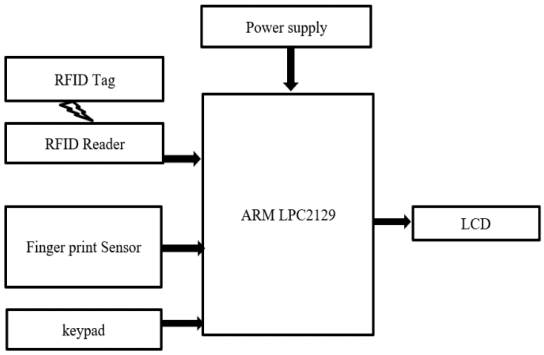

Fig-1: Block diagram of proposed model

IV.DESCRIPTION

Biometrics refers to the use of technology to measure and evaluate biological information. With the increasing use of electronic communication, biometric data can be accessed and used to introduce services using electronic devices. This technology can be used to enhance the voting process by recording and storing election data as digital information. In the past, data security was overseen by the ministry of defense and federal government instructions. Various human body segments such asDNA, voice patterns, hand patterns, and finger prints can be used for authentication. Biometric voting systems utilize these patterns to authenticate and identify voters, ensuring enhanced privacy and security. One such system is the thumb impression scheme, which uses the uniquethumb impression of individuals to authenticate and identify them. In countries like India, a thumb impression database has been created for users via the Aadhar database. This database can be used to identify instances of repetition or illegal cases. Voters do not need to register their fingerprints in the election booth, as the technology behind fingerprints is utilized to establish the whole scheme. The aim of the project is to establish a system that requests users to providetheir fingerprint as an identification proof

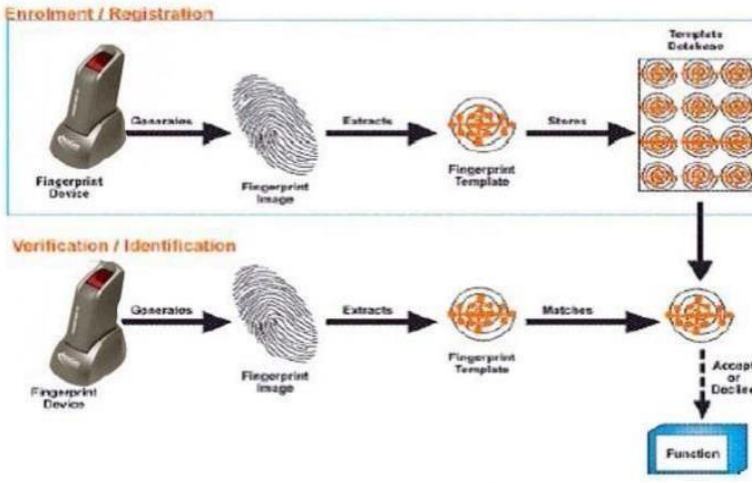

Fig 2: Fingerprint registration

The fingerprint-based voting framework works by encoding the unique fingerprint pattern of a voter and comparing it to the information that has been stored in the database. If the pattern exists in the database, it can be matched with the past stored information. This authentication process allows voters to enter the system and cast their votes. One of the advantages of this system is that it can identify false users who may try to cast votes illegally. This helps to maintain the integrity of the voting process and ensures that the rights and identity of citizens are protected. By using biometric data such as fingerprints, the

system can provide enhanced security measures and prevent fraudulent activities. Overall, the use of biometric data in voting frame works can help to ensure fair and secure elections. It provides an accurate and efficient means of authentication and identification, allowing voters to participate in the democratic process with confidence.

V.COMPONENETS OF THE MODEL

Radio Frequency Identification model

RFID technology has a wide range of applications, and one of the most common uses is for tracking and inventory control. By attaching RFID tags to products, companies can track the movement of their inventory in real-time, which helps them to manage their stock levels more effectively and reduce the risk of theft or loss. RFID technology can also be used to automate the process of checking items in and out of a library, for example, or to monitor the location of items in a warehouse or factory. Additionally, RFID technology is used in a variety of other applications, such as asset tracking, supply chain management, and even in healthcare for tracking patient records and medical equipment.

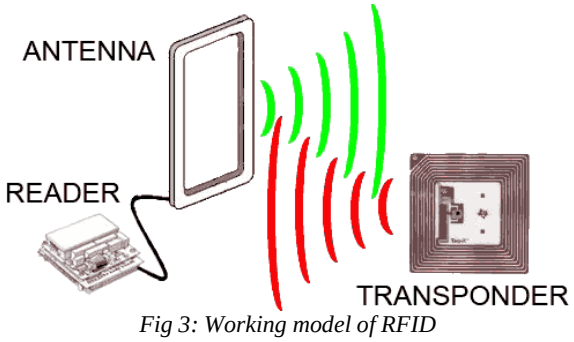

Fig 3: Working model of RFID

Arduino

Arduino is an open-supply electronics platform that offers an easy-to-use hardware and software program answer for constructing digital projects. Arduino boards are designed to read inputs and turn them into outputs based on a set of instructions provided by the user. The Arduino programming language is based on Wiring, andthe Arduino Software (IDE) is based on Processing, which makes it easy for users to get started with programming and building electronic projects. The Arduino platform has become very popular among students, hobbyists, artists, programmers, and professionals who want to build electronic projects for various applications. The platform has a large and active community of users who share their knowledge and expertise, which has led to the development of thousands of projects and contributed to the growth of the platform. Arduino was originally designed as a tool for fast prototyping aimed at students without a background in electronics and programming. However, as the platform became more popular, it started to evolve and adapt to new needs and challenges. Today, Arduino offers a wide range of boards and products that cater to various applications, including IoT, wearables, 3D printing, and embedded systems. One of the key features of Arduino is that it is completely open-source, which means that users can build their own boards and adapt them to their specific needs. The software is also open-source, and it is continually growing and evolving through the contributions of users worldwide.

Biometric System

The fingerprint module scheme is an input device that is used for processing fingerprints. It includes two parts: fingerprint enrollment and fingerprint matching. During the enrollment process, users are required to feed in theirfingerprints twice. The system then processes the two-time fingerprints and produces a template of the fingers based on the processed results and the templates. The process of matching fingerprints involves computing fingers using optical systems and sensors, which then produce a template of fingers before comparing it with a number of templates in the finger libraries. The system will contrast the live fingers with the patterns that are stored in the database. This will then search the system for collected matched fingerprints. The main aim of this system isto enhance security and privacy in the voting process. The matching fingerprints are collected and stored in the database, and the exact patterns are locked to avoid fake casting of votes. By using this system, it is possible to ensure that only legitimate voters are able to cast their votes, and that the voting process is fair and transparent. The results and procedures of the system have been tested and found to be effective in ensuring secure and accuratevoting.

Fingerprint Enrollment and verification

The use of biometrics, such as fingerprint scanning, can greatly enhance the security of voting systems. By requiring second-stage authentication and matching the fingerprint of the voter with the database, it becomes much more difficult for someone to cast an illegal vote. The uniqueness of each individual's fingerprint also makes it a highly reliable method for identification and authentication. The use of microcontrollers can also help to simplify and streamline the voting process, making it moreaccessible to people in various locations and with different levels of technological infrastructure. However, it is important to ensure that the use of such technology does not lead to a loss of privacy or personal data. While some countries may still use traditional paper ballots, it is important to recognize that the implementation of advancedvoting technologies can greatly enhance the security and accuracy of the voting process. Ultimately, the goal should be to create a voting system that is both secure and accessible to all eligible voters.

Fig 6: Fingerprint enrollment and verification

VI.CONCLUSION

The proposed implementation of a fingerprint-based voting system using RFID and the Internet of Things(IoT) is a promising solution for ensuring accuracy and fairness in the voting process. By using fingerprint recognition techniques, the system can prevent fake votes and unauthorized individuals from casting their votes. The use of IoT enables real-time management of the system, providing greater efficiency and transparency. Additionally, the system ensures privacy and confidentiality of the voters' identities, further enhancing the security of the voting process. The inclusion of a buzzer to alert the presiding officer in case of any unauthorized attempts to cast votes is a valuable feature, adding an extra layer of security to the system. The high accuracy of the system and the fact that only eligible candidates can cast their votes ensures fairness and impartiality. It is commendable that the proposed system has been designed to cater to physically challenged users, making it inclusive and accessible to a wider range of individuals. Overall, the implementation of a fingerprint-based voting system using RFID and IoT has the potential to revolutionize the voting process, enhancing its security and reliability while ensuring fairnessand inclusivity.

VII.FUTURE WORKS

It is true that using face identification-centered retinal scan process can provide a high level of authentication accuracy. However, it is important to note that such technology may not be easily accessible or affordable for all populations. Additionally, connecting the voting scheme to AADHAAR or any other database raises concerns about privacy and data security. It is important to ensure that any such connections are made with appropriate safeguards in place to protect user data.While IRIS technology can provide effective results for authentication, it is important to consider the user experience and accessibility of such technology. For example, some users may have difficulty positioning their eyes correctly for scanning, which could lead to errors or delays in the voting process. It is important to ensure that any technology used in voting systemsis accessible and user-friendly for all voters, regardless of their abilities or technical expertise.

References

[1] *Surendra Rao B Prasanth E Siva Sai Teja R Sandeep Y 2019, RFID based Smart Voting SystemInternational Research Journal of Engineering and Technology 6(4), 1577-1580*

[2] *Kiruthika Priya V VimalaDevi V Pandimeenal B and Dhivya T 2017, Arduino based Smart Electronic Voting Machine InternationalConference on Trends in Electronics and Informatics*

[3] *Abdulkadir H Alkali Emmanuel G Dada Dauda E Mshelia Sadiq O Onundi 2019, Design and Development of an Arduino Based Electronic Voting System International Refereed Journal ofEngineering and Science 8(1), 48-57*

[4] *Sudhakar M and B. D. S. Sai B D S 2015, Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller IOSR-Journal of Electronics and Communication Engineering 10(1),57-65*

[5] *Prasad M R Bojja P and Nakirekanti M 2016, AADHAR based Electronic Voting Machine using Arduino International Journal of Computer Applications 145(12), 39-42*

[6] *Venkateswarlu M and Kumar Y V V 2014, Biometric System Based Electronic Voting Machinewith security algorithm and password protection onARM Microcontroller and GSM International Journal of Science Engineering and Advance Technology 2(7), 197– 200*

[7] *Kumar M D Santhosh A Aranganadhan N S andPraveenkumar D 2016, Embedded System based Voting Machine System using Wireless TechnologyInternational Journal of Innovative Research in Electrical, Electronics, Instrumentation And ControlEngineering 4(2), 127-130*

[8] *Prabha R Trini X Deepika V and Iswarya C 2016, A Survey on E-Voting System Using ArduinoSoftwareInternational Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering 5(2).*

[9] *Chitti S and Samyuktha L 2019, Data acquisition of greenhouse gases and energy monitoring system using GSM technology International Journal of Innovative Technology andExploring Engineering 8(6S4), 820-825*

[10] *Swapna A and Arun Kumar J T 2019, Securedvehicle safety system using GSM technology International Journal of Innovative Technology andExploring Engineering 8(6s4), 832-836*

[11] *Arabelli R R and Revuri K 2019 Fingerprint and Raspberri Pi based vehicle authentication andsecured tracking system International Journal of Innovative Technology and Exploring Engineering 8(5), 1051-1054*

[12] *Kumar V and Anuradha P 2019, Power consumption optimization and home automaton using smart sensor networks International Journal ofInnovative Technology and Exploring Engineering 8(6S4), 837-841*

[13] *Kumar M A 2019 Security and controlling system at home by using GSM technology International Journal of Innovative Technology andExploring Engineering 8(9), 2471-2474*