ISSN: 2278-4632
Vol-13, Issue-06, No.01,June : 2023

AADHAAR-BASED ELECTRONIC VOTING MACHINE USING FINGERPRINT AUTHENTICATION

T.Madhan Kumar, P. Bhanu sai Prakash, P. Akshay Kumar, Student, Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad, India.
V.S.G.N. Raju, Assistant Professor, Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad, India.

Abstract—
Fingerprint scanning technology for authenticating real voters can be integrated into existing systems. Electronic Voting Machines (EVMs), by which fraud voters can be eliminated. This is a safer and more convenient device for security rather than manual verification that is vulnerable. Authentication plays a very major role in EVMs, in regard the Fingerprint scanner interfaced with the embedded system recognizes genuine voters and are allowed them to cast their vote for their desired candidate through a small keyboard interfaced with the same system. The keyboard marked with party symbols and candidate names avoids confusion, by which the activated favorite key information will be stored in the embedded system. This keyboard contains four keys and the voter can select the suitable candidate by choosing the corresponding key. Polled votes information will be stored in the internal RAM of the Arduino. The Arduino is programmed to accept the voter choice only once, after that the system regrets to acquire activated key information and the door of the keyboard will be closed automatically after the vote has been polled. The voting process has been streamlined thanks to biometric voting. It is a cutting-edge method that is preferred over conventional EVM voting because it is potentially flawed. It is helpful since it has advantages like avoiding invalid votes (booth capturing), cutting down on counting time and costs associated with staff deployment, as well as maintaining voter photo ID cards for identification.
Keywords-*Arduino, Authentication, Electronic Voting Machine (EVM), Booth Capturing.*

I. Introduction:

The purpose of this project is to present the issue of highly secure biometric voting by documenting the design, development, and manufacture of a single project demonstration unit. There are several methods for developing electronic voting machines across the world. The vast majority of voting devices are constructed using computers or microcontrollers. The project's electronic voting system is built with biometric technology, a fingerprint scanner, and an Arduino UNO board.
This report provides an introduction to voting technology, which is expanded on in the following chapters, in order to introduce the topic of electronic voting and provide some historical context. Please begin by providing a brief explanation of the two technologies employed in the project, specifically the biometric fingerprint module.

Biometric Technology

Biometric technology is a relatively new and imaginative technology that is frequently used in safety and security applications. Fingerprint scanning time technologies are one type of biometric technology that is commonly used in safety and security applications. Fingerprint scanning is one type of biometric technology. First and foremost, we must comprehend biometric technology. This approach is described in more detail below.
Biometrics can automatically recognize a person based on physical or behavioral characteristics A biometric system is essentially a pattern recognition system that certifies the validity of a particular physiological measurement or behavioral attribute that the user possesses. As a result, "biometric technologies" refer to "automated methods of identifying or authenticating a living person's identity based on a physiological or behavioral characteristic."

Copyright @ 2023 Author

ISSN: 2278-4632
Vol-13, Issue-06, No.01,June : 2023

II. Literature review:

Existing method:

The existing system for voting in many countries typically involves the use of paper ballots, where voters mark their choices on a paper ballot and deposit it in a ballot box. The ballot boxes are then collected and transported to a central location for manual counting.

While this system has been used for many years, it is not without its challenges. There is a risk of ballot tampering, and the manual counting process can be slow, leading to delayed results. Additionally, using paper ballots can be environmentally unfriendly and lead to logistical challenges in transporting and storing the ballots.

Electronic voting systems, such as evms, have been developed and implemented to address these challenges in many countries. Evms have the advantage of speed, accuracy, and ease of use, with votes being counted electronically, reducing the risk of manual errors. However, evms have been subject to criticism due to concerns about their security and transparency, with some experts suggesting that they can be vulnerable to hacking and manipulation.

Proposed method:

To address these concerns, some countries have implemented additional security measures, such as paper trails and audit logs, to safeguard the voting process's integrity. However, the use of fingerprint authentication, as proposed in this project, could provide an additional layer of security and transparency, further enhancing trust in the voting process.

This project's primary goal is to entirely avoid rigging. To avoid election rigging to the fullest extent possible, electronic voting technologies have been implemented. However, there could be some errors during elections. As a result, an electronic voting system based on fingerprints has been developed. A person must provide all of his information and an image of his fingerprint in order to register himself as a voter. As a result, in order to poll his vote during an election, the same person must first provide a fingerprint image. As a result, the system scans his fingerprint and matches it to one that has previously been recorded. The person can enter the room to cast his vote by opening the door if both images match.

III. Methodology

A) *Block Diagram*

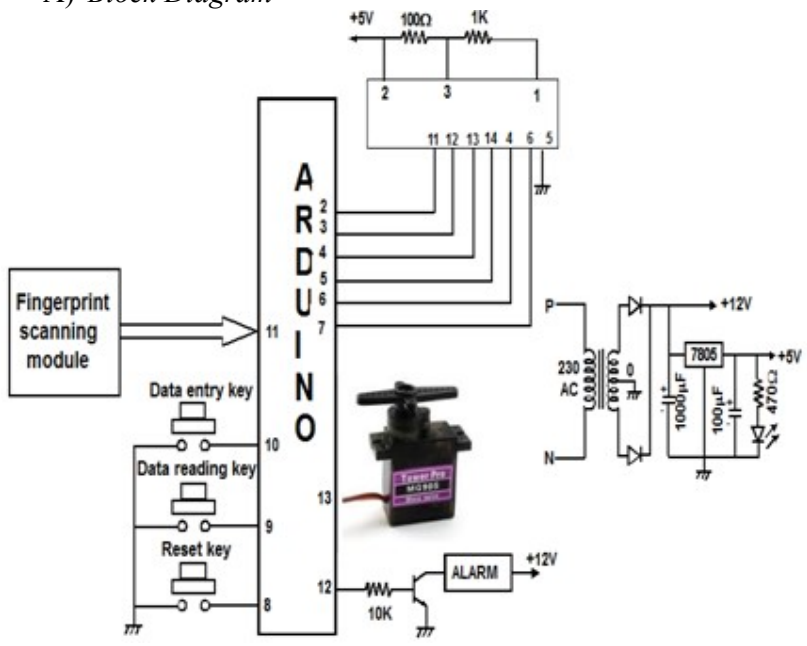

Fig 1. Block Diagram

Copyright @ 2023 Author

ISSN: 2278-4632
Vol-13, Issue-06, No.01,June : 2023

B) Hardware Specifications

1. Arduino board

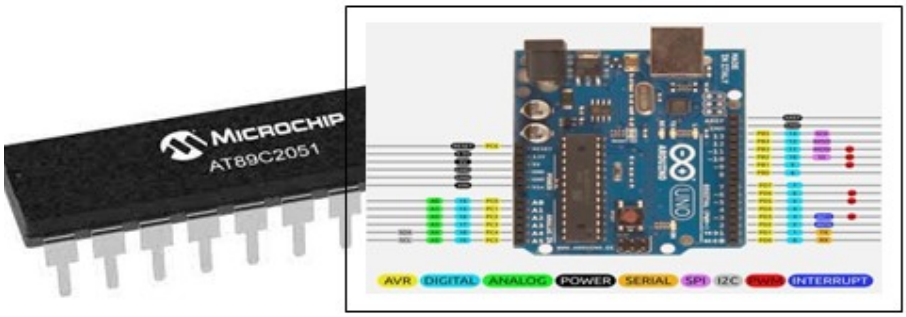

Fig 3.1 Arduino Board

2. Fingerprint Module

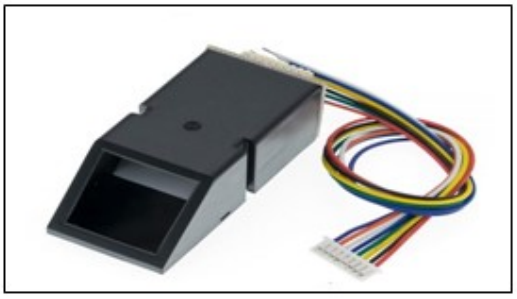

Fig 3.2 Fingerprint Module

3. LCD Display

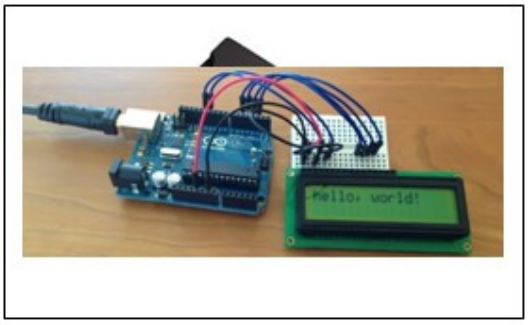

Fig 3.3 LCD Display

4. 7805 – Voltage Regulator

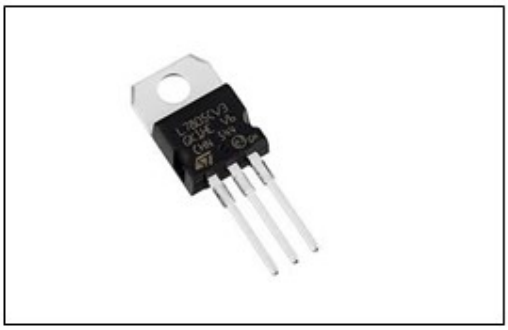

Fig 3.4 7805 – Voltage Regulator

5. Servo Motor

Copyright @ 2023 Author

ISSN: 2278-4632
Vol-13, Issue-06, No.01,June : 2023

Fig 3.5 Servo Motor

6. Buzzer

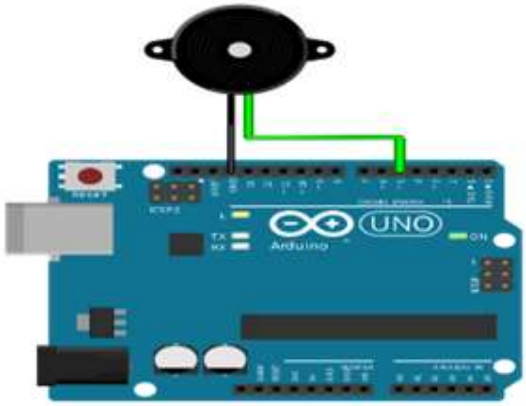

Fig 3.6 Buzzer

7. Transformer

Fig 3.7 Transformer

8. Push button

Fig 3.8 Push button

ISSN: 2278-4632
Vol-13, Issue-06, No.01,June : 2023

IV Working

The process of execution:

1. Initialization Upon startup, the Arduino Uno initialises the LCD, servo motor, and fingerprint module. The LCD instructs the user to enrol their fingerprint or authenticate using a fingerprint that has already been registered.

2. Enrolment: The user clicks a push button to register their fingerprint, causing the device to start taking pictures of it. The system maintains the fingerprint template after it has been recorded and creates an enrolment code for that fingerprint. A message stating that the enrolment was successful is displayed on the LCD.

3. Authentication: The user hits a different push button to authenticate using their previously registered fingerprint. If the fingerprint matches with the already enrolled fingerprint, then the gate open and the voter can go inside the polling booth to vote for their representatives.

4.Vote casting: Once the user presses the button, the system records their vote in a database or a local memory.

5.Vote count: The system keeps a count of the number of votes cast for each candidate and displays the results on the LCD.

6.. Repeat: The user can enrol additional fingerprints or authenticate with their enrolled fingerprints as needed, using the same process.

V Hardware Arrangement

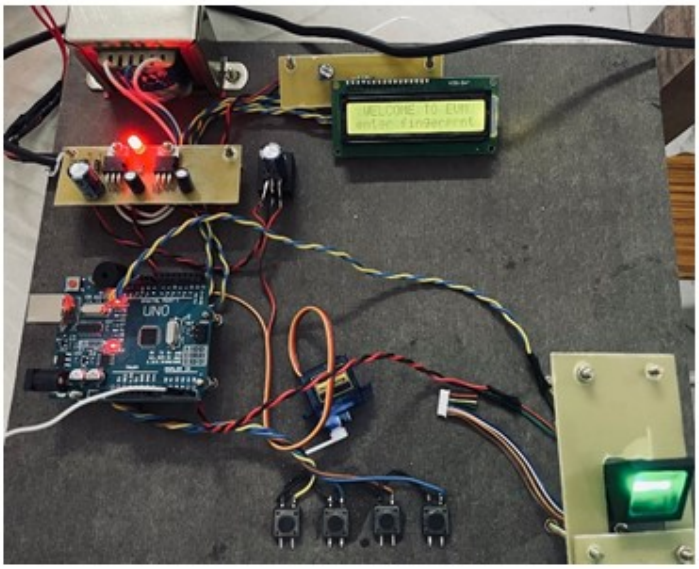

Fig 5.1 Hardware setup

Copyright @ 2023 Author

ISSN: 2278-4632
Vol-13, Issue-06, No.01,June : 2023

VI Results

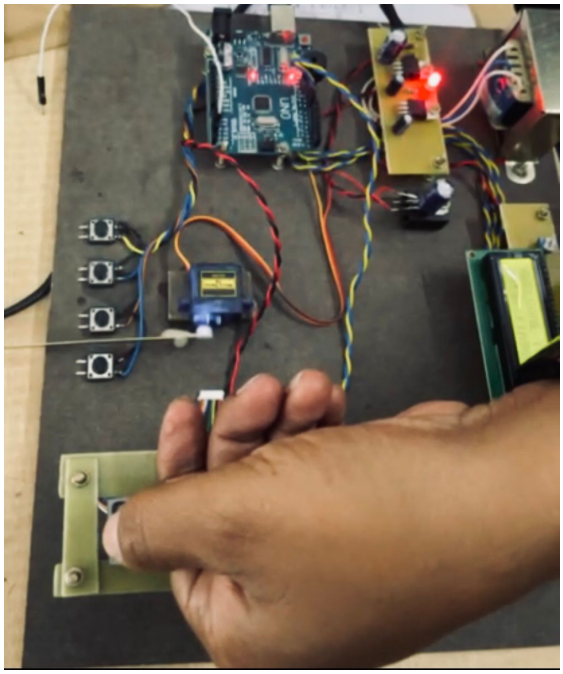

Fig 6.1: While biometric authentication

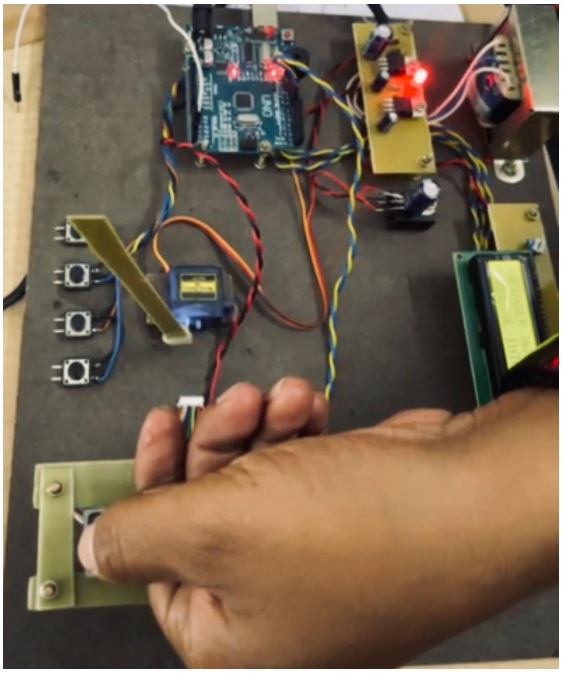

Fig 6.2: After successful authentication

VII Advantages and Applications

ADVANTAGES

1. Improved security: fingerprint authentication provides a high level of security, ensuring that only authorized individuals are able to cast their votes.
2. Accurate vote counting: the system accurately records and counts votes, reducing the likelihood of errors and ensuring the integrity of the voting process.
3. User-friendly interface: the LCD and push buttons make the system easy to use and navigate, even for individuals who may not be familiar with the technology.
4. Flexibility: the project can be adapted to a variety of applications, including door locks, attendance systems, and other security and authentication systems.
5. Cost-effective: the project is relatively low-cost, using widely available and inexpensive off-the-shelf components.
6. Time-saving: the project saves time by eliminating the need for manual vote counting, attendance tracking, and other tasks that can be automated using fingerprint authentication.
7. Scalability: the project can be scaled up or down to accommodate different numbers of users or voters, making it suitable for a range of different applications.

APPLICATIONS

1. Elections: the project can be used to create secure and reliable electronic voting systems that accurately record and count votes.
2. Security systems: the project can be used to create secure door locks, access control systems, and other security systems that require user authentication.
3. Attendance systems: the project can be used to create attendance systems that track and record employee or student attendance using fingerprint authentication.
4. Banking and finance: the project can be used to create secure authentication systems for online banking and financial transactions, improving security and reducing fraud.
5. Government and public services: the project can be used to create secure identification systems for government services such as tax collection, public transportation, and other public services.

Copyright @ 2023 Author

6. Education: the project can be used to create secure student identification and attendance tracking systems in educational settings, improving student safety and reducing errors.

VIII Conclusion

In conclusion, the "EVM with Fingerprint Authentication" project is a highly innovative and useful project that addresses several key challenges associated with voting systems. By combining advanced technologies such as fingerprint authentication, LCD displays, and servo motors, this project is able to create a highly secure, reliable, and efficient voting system that can be customized for a wide range of different applications. With its low cost, ease of use, and scalability, this project has the potential to revolutionize the way that voting is done in many different contexts, improving security, reducing errors, and saving time and resources. Overall, this project represents an exciting example of how technology can be harnessed to create innovative solutions to real-world problems.

- The use of fingerprint authentication technology makes this project highly secure, as fingerprints are unique to each individual and cannot be replicated or stolen easily.
- The LCD display used in this project provides a clear and easy-to-read interface for users, making it simple to navigate and use.
- The servo motor used in this project ensures accurate and reliable movement of the mechanical parts, ensuring that the system operates smoothly and efficiently.
- By automating the voting process, this project eliminates many of the errors and inaccuracies associated with manual vote counting, making it more reliable and accurate overall.
- This project is also highly adaptable and can be customized to meet the specific needs of different applications or contexts.
- Finally, this project has the potential to improve voter participation and engagement, by making the voting process more accessible and convenient for users.

Overall, the "EVM with Fingerprint Authentication" project is a highly innovative and useful project that has the potential to revolutionize the way that voting is done in many different contexts, improving security, accuracy, and efficiency, while also making the voting process more accessible and convenient for users.

REFERENCES

[1] Linear Integrated Circuits By: D. Roy Choudhury, Shail Jain
[2] Digital Electronics. By JOSEPH J. CARR
[3] Fundamental of Radio Communication: By A. SHEINGOLD
[4] Digital and Analog Communication System By: K. sam Shanmugam
[5] Electronic Circuit guide book Sensors by JOSEPH J. CARR
[6] E. Arts and S. Marzano, The New Everyday: Views on Ambient Intelligence, 010 Publishers Rotterdam, 2003.
[7] Ross Anderson and Markus Kuhn, Tamper Resistance a Cautionary Note, in Proc. 2nd USENIX Workshop on Electronic Commerce, 1996.
[8] Ross Anderson and Markus Kuhn, Low-Cost Attacks on Tamper Resistant Devices, in Mark Lomas (ed.), Security Protocols: 5th International Workshop, Paris, France.
[9] California Internet Voting Task Force. “A Report on the Feasibility of Internet Voting”, Jan.2000. [4] Chaim D., “Secret-ballot receipts: True.
[10] S.N. Chandra Shekhar, Dr. Avinash Gour, Dr. S P V Subbarao " Performance Analysis and Capacity Enhancement of MIMO-OFDM system for Multi Media Transmission " TEST Engineering and Management, Volume No.83 Page No.27101-27108, ISSN:0193-4120, April-2020.
[11] S.N. Chandra Shekhar, Dr. Avinash Gour, Dr. S P V Subbarao " Performance Analysis and Capacity Enhancement of MIMO-OFDM system for Multi Media Transmission " Journal of Critical Reviews, Volume No.7, Issue No.15, ISSN:2394-5125, July-2020.

s

 Copyright @ 2023 Author