IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 3, May 2022

Implementation of Smart Election System using IoT

V. Revathy, V. Rubika, M. Sadhana, Ms. K. Arthi

Department of Electronics and Communication Engineering

SRM Valliammai Engineering College, Kattankulathur, Tamil Nadu, India

Abstract: *In Indian Democracy, Voting is the essential fundamentals of each citizens. Building a secure balloting system has been a challenge for a due course of time. In this modern scenario, vote casting system has a few troubles with it. One of the most important problems in existing vote casting system EVM (Electronic Voting Machine), is confidentiality of voter, loss of secrecy of ballot, voter anonymity etc. In this paper, we proposed a biometric method which will resolve the problem of the modern-day voting system. Here, we added the concept of getting the fingerprint impact of a voter which is entered as input to the system. Then, compared with the collected information in the database. If the precise pattern suits with the reachable record, then casting a vote is permitted. Then the quick result is on the spot and counting is performed by means of IoT.*

Keywords: Smart Election System, IOT Fingerprint Scanning; Robust, User Friendly

I. Introduction

Democracy has given people a right to make their choice. So, to have remarkable vision we want to take right decision. This can be made by "voting". The traditional voting mechanisms follows the problem of voter identity and other Information which is generated manually. So, there are possibilities of parallax errors.

To extend the efficiency and accuracy of vote casting procedures. Large number of computerized voting systems have been developed to assist accumulating and counting the votes. Which consist of Lever Voting Machines, Voting based totally Punched Cards and Optical Mark- Sense Scanners and Direct Recording Electronic (DRE) voting systems.

Even though, we are having many technologies, those type of advanced and developed technology has some disadvantages. The electronic voting machine currently in usage additionally has few disadvantages. Voter can hear the sound produced by the electronic vote casting machine, however the man or woman no longer getting acknowledgement after the voting. And also the man power is required to perceive the person`s identity.

Moreover the digital balloting machine devised in a such a way results in misconceptions like people whomever they vote, will be converted into some other's party or candidates. It can also be misused. To avoid this type of drawbacks our proposed architecture had been developed.

In this paper, we have designed an Implementation of Smart Election system using fingerprint authentication and centralized database with the help of IOT which has better protection and innovative advancements. Furthermore, the system is relevant to use anywhere in the world.

We arrange the rest of the paper as follows. Issues in the present systems are discussed in Section II. In Section III , we present the proposed idea of the system. Methodologies and System Implementations are mentioned in Section IV. Section V states the working concepts while, Section VI focuses on the result analysis and future plans. Finally, Section VII concludes the paper.

II. Existing System

At present, voting process are primarily based on Electronic Voting Machines and Secret Ballet Voting which requires man-power and are time-consuming processes. This type of structures has lot of drawbacks like 1)Voter’s Id and others details are validated manually and only after affirmation he/she will be allowed to vote.2)EVMs have to checked and transported anywhere the election is taking place which needs manual work and security.3)The counting of the votes casted in EVMs additionally wishes manpower and takes a complete day.4)In EVM, there is no module that can confirm if the citizen’s votes are solid or not.5)And, the ballot system of voting is absolutely manual which has lot of misconceptions and so on. Hence, the proposed architecture can be made a lot better with more accessible and greater efficient.

DOI: 10.48175/IJARSCT-3735

2.1 Existing Voting Techniques

The problems that are located in the existing systems are multiplied costs, single factor of failure, and the message which not verify that the vote is registered for the voter's favourite candidate to whom he/she had forged the votes. There is a possibility that the voter's vote is registered to some other candidate as a substitute than the one who he had casted and also excessive opportunity of misconceptions and malpractices. Mainly safety is missing in this type of current systems.

A. Electronic Voting Machine

EVM is made up of two units- manage unit and balloting unit and these two are connected with the help of a five-meter cable. These provide the voter with a button for every preference which is connected by using a cable to an electronic ballot box. When a voter presses a button against the candidate he/she wishes to vote for, the machine locks itself. This function of the EVM ensures that one voter solely votes once.

As far as the hazards have been concerned, EVM malfunctioning all through the election procedure suggested resulted in some inherent defects in a precise machine. Also, the EVM tampering is intentional and is no longer backed via any evidence so far being viable.

B. Anti-Fraud Voter Registration and Voting System Using Data Card

A technique for figuring out fraudulent voting that includes the use of wallet-size cards having a permanent facts storage medium and a brief statistics storage medium disposed on every card. A first card writing device acquires biometric facts from a character and is used for writing a template that records the permanent storage medium. A voter registration verification terminal acquires the biometric information from a possessor of that card, and additionally reads the biometric records from the permanent storage medium of the card. Upon inputting biometric facts from each the card and the possessor of the card, the verification terminal compares the information, and, if they match, writes data permitting constrained use of the card for vote casting on the brief data storage medium of the card. This information can be read at voting terminals at different locations.

The issue on use of the card for balloting and the required repeated verification enhances protection of the cards, the voter registration, voting terminals and systems

C. Ballot Casting Assurance with the Aid of Voter-Initiated Poll Station Auditing

Voters and other fascinated parties at a polling station uses an interactive ballot encryption machine to attain one or more encrypted ballots. No identification is integral to use these ballot encryption devices, and they may be used as many instances as favoured with the aid of any individual. Subsequently, eligible voters votes that are casted encrypted ballots by way of identifying themselves to poll employees through a sign-in manner and supplying one of the encrypted ballots produced via a ballot encryption device. Any uncast ballot can be opened to grant assurance as to its legitimacy.

But the foremost disadvantage of this device is that, a coercer might also be capable to view the contents of an encrypted ballot with the aid of forcing a voter to open it as an alternative. A coercer right here refers to the vote- buyers.

2.2 Literature Survey

In the paper [1], The system has a double verification and also uses a cloud database; The GPS in the system, will prevent the system from theft. And also if the system has been stolen it can be located easily with the help of satellites. Through GSM module, we can get a confirmation message ,that a candidate vote got registered or not. This way the elector can verify that the voter is pitched to his candidate. Even though, It is not suitable for small scale and voter's current situation about voting process was quite complicated

The Smart online voting method is used to develop a secure internet voting system based on face recognition which tried to overcome all the drawback occurs in traditional or current voting system. The system has many strong features like correctness, verifiability, convenience etc. Only the internet connection and face scanners are required in this voting system [2]. This system uses facial recognition, it causes potential drawbacks like threats to privacy, errors and slow recognition leads to delay in the voting process

The Biometric based secure remote voting system has been devised to propose a feature that will link the Aadhaar database of Unique Identification Authority of India (UIDAI), Govt. of India, New Delhi; can be embedded [3]. This system facilitate

DOI: 10.48175/IJARSCT-3735

all the voters to get registered on the portal automatically, which are classified on the basis of regions and constituencies by using their unique identification i.e. their finger prints. This method may not survive due to the complication and the malfunctions in the machine leads to adverse effects in the voting process.

The E-voting system uses 2-factor Bio-metric authentication Face recognition using Eigen face-based recognition algorithm is used and Minutiae based algorithm with a database as an input which is advanced compared to the traditional form of voting process [4].This computing process has better protected software and avoid the chance of misconceptions and fraudulence activity. The system has limitations such as, it will becomes susceptible to delays caused by network congestion.

The E-voting method proposes uses bio metric identification system using fingerprint scanner which is interfaced with the vote casting machine[5]. Raspberry Pi technology has been used which acts as the database for the information of the voter and acts as a storage of vote counts. Once the candidate places his/her finger, the Raspberry Pi checks with the records in the database for the records of the voter. Only when the fingerprint matches corresponding to the placed in the reader the machine opens the voting process. This biometric system combined with raspberry pi is not as much faster and it is a time consuming process. It is not much compatible for the voting system.

In the Electronic voting biometric system, they are using combination of hardware and software. Raspberry Pi 3B+ (RPI) is a hardware device connected to the Fingerprint Scanner, Touch Display. It acts as a storage for the data on the cloud[6]. The voter will enter the aadhaar-id on Touch screen module, and then fingerprint of voter will be scanned that will be matched with database saved on the cloud. If it matches, then only in addition process will start. The Candidate has to select his region. Now, voter is able to cast his vote. After casting the vote, the vote depend of that candidate will be incremented. The vote count number is encrypted and saved quickly in the machine memory. Encrypted vote count number is then saved on the cloud. After vote Casted are increment, the Candidates disable request will be given to database, so as to avoid the multiple number of voting.

The ESVS [7], is kind of vote casting system which candidate can grant access to execute their individual voting rights. Oracle 9i has been used as a database server. This tool is implemented by using java and exposes a GUI to person who can process to create and delete the database when required. The voting details enabled by user using GUI is executed and encrypted in Java and collected in Oracle database. ESVS uses aadhar number to authenticate the candidate through OTP. These biometric authentication allows people to cast their votes using smart phones. It will reduce time consumption during election and increase the percentage of voting capabilities.

The Online Voting system using cloud platform offers smart tickets, super agenda highlights, vote counting, classification and revealing [8]. These capacities are programmed and do not need to be doled out to faculty in- house. Furthermore, it allows heads to make decides on polls with the purpose that voters cannot solid invalid votes, nor do they need to be checked while tallying. The Online Voting Platform presents the least disturbing and most helpful approach for administrators and voters alike. For directors, the way toward placing up a ticket and leading a choice is basic and sensible.

III. Proposed System

Our Proposed System is a finger-print based system application that enhances our us of a with a better vote casting device to make certain a hundred percent voting. Since the existing vote casting gadget is not having high safety our task will overcome this main drawback.

3.1 Proposed Idea of the System

This proposed system is much better protected and work with higher efficiency than the system that is already present. This system includes a database that has a list of the voters who have cast their votes. This list is provided in order to determine the voters one's who wasted their valuable chance to decide the rightful candidate representative and the corresponding steps or measures can be taken regarding these default voters

The major purpose of this challenge is to make a vote casting system designed with the use of fingerprint technology to provide a secured form of voting. The proposed system architecture is shown in Fig. 1. A centralized database is maintained where the records of all the citizens is collected. Whenever a citizen cast his vote, his/her data and fingerprint is verified and authenticated with the data existing in the database.

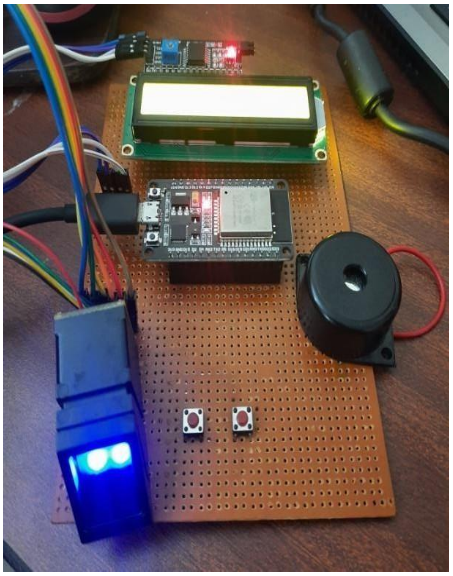


Figure 1: Architecture of the proposed system

If the data stored in the database doesn't suit with the voter's Information then he/she is not allowed to vote. If the records match, the system tests for double voting. If the voter has already voted once, he/she is no longer allowed to vote once more else the voter is allowed to cast his/her vote .In the technique of voting, voicing their preferences or articulating views. As the world is altering day by means of day and is critical to adapt to the digital world in order to survive and meet world standards

3.2 Hardware Description

1. **Fingerprint scanner:** A fingerprint scanner is a sort of device that recognizes and validates the fingerprints of a distinct in order to permit or refuse entree to a Process or a bodily facility. It is a kind of biometric protection tools that features with the arrangement of hardware and software procedures to discover the fingerprint images of a distinct. It typically operates by way of firstly storing fingerprint images of all approved persons for a specific system or device. These images are held again inside a database. The person requesting for to place their thumb on a fingerprint sensor, which senses and grant the replica fingerprint of the specific citizen and search for correspondence with the main database and cross-checks with the previously saved images. Solitary if there is any positive contest, the individual is approved for an entrance or access. In this project, fingerprint scanners are used for verification functions so that the vote casting technique can be more secure.
2. **ESP32 Microcontroller:** The ESP32 is a very versatile System On a Chip (SOC) that can be used as a generic purpose microcontroller with quite an giant set of peripherals which includes Wi-Fi and Bluetooth wireless capabilities. Most ESP32-based designs use pre-made modules that consist of an genuine ESP-32 SOC, exterior flash memory, and a crystal and pre-tuned PCB antenna or an IPEX antenna connector. One large benefit to the use of this module is that it has already pre-loaded the low-level device drivers, the wireless protocol stacks for Wi-Fi b, g, n, Bluetooth and BLE, and Free RTOS as the base OS. In addition, a boot loader has additionally been loaded to allow for noticeably convenient downloading of user applications. It allows direct connection to a computing device PC that can then be used to compile, download, and run packages directly on this module. It allows you to do ADC conversions, computation, and level thresholds while in deep sleep.
3. **I2C Protocol:** The Inter-Integrated Circuit (I2C) Protocol is a protocol supposed to enable more than one "peripheral" digital built-in circuits ("chips") to talk with one or greater "controller" chips. It is a serial communication interface with a bidirectional two-wire synchronous serial bus commonly consists of two wires – SDA (Serial data line) and SCL (Serial clock line) and pull- up resistors. They are used in projects that require many distinct components (e.g. sensors, pin, expansions, and drivers) working collectively as they can connect up to 128 units to the main board whilst retaining a clear conversation pathway. It is used to connect a variety of low-speed

DOI: 10.48175/IJARSCT-3735

devices collectively like microcontrollers, EEPROMs, A/D and D/A converters, etc.

4. **LCD Display Screen:** LCD is a liquid crystal display used to produce a visible image. They have become very frequent and have taken a large leap in the screen industry by actually changing the use of Cathode Ray Tubes (CRT).LCD's have made shows thinner than CRT's. Even while evaluating the LCD display to an LED screen, the energy consumption is lesser as it works on the simple principle of blocking light rather than dissipating. Liquid crystal displays are super-thin technology display monitors that are typically used in laptop screens, TVs, mobile phones, and portable video games. In this project, the LCD display is used to bring the relevant data to the user. Mainly, when the voter has voted it will display the name of the voter who has casted his vote. Similarly, when the voter has casted his vote already tries to forged vote again means a buzzer gets activated and the LCD will display the present voter had already forged his vote beforehand, and also when the voter information does not suit with the fingerprints scanned that time also it will exhibit the textual content that there is no match and when there is any different error takes place during voting process, it will exhibit the text correspondence with the error.
5. **Buzzer:** The buzzer is a sounding device that can convert audio signals into sound signals. It is normally powered via DC voltage. It is extensively used in alarms, computers, printers and different electronic products as sound devices. .It is an extraordinarily small and stable two-pin device as a result it can be simply utilized on breadboard or PCB. In this project, the buzzer is active when there is any error happens at some point of the vote casting system such as when a voter who already voted try to forged vote again, when the voter information, as well as fingerprints, does not match, and when any other error occurs.
6. **Push Button:** A push button typically stimulates a change in the circuit or produces an output when the button is usually pressed. It is made up of plastic or metallic and flat surfaced to be effortless to press. These types of switches are also known as momentary switches. Based on the utilization the typical size of the buttons varies. For emergencies generally a red push button of reasonable sizes are used.

There are some industrial purposes where when one push button is pressed the other pops out. To keep away from the conditions where the user presses the inappropriate button these buttons are colour coded. Here two push buttons are used in this project each having a separate functionality. One is to pick out the first party, and the another push button is for the other party whom they wanted to vote.

IV. Methodology

This complete methodology discusses about the Biometric primarily based voting system .As we comprehend Biometric is one of the special identity like DNA, fingerprint and Iris. In this Proposed system, we have used the Biometric verification approach to beautify the safety and protection of voting process to avoid malpractice in the course of elections. The components used are

- Fingerprint sensor
- Esp32 microcontroller
- I2c driver
- LCD Display
- Buzzer

The voter's database will be saved in the server. The database may consist of the whole Name of the voter, Age of the voter, Biometric information of the voter. There are no storage gadgets included in the vote casting device. All the storage or reminiscence is inside the server. IOT Technology is used for the server operations and to replace the vote casting details.

The above block diagram describes the entire systematic architecture of our proposed system. Input devices include fingerprint scanner, push buttons which denotes the parties of the election and the output devices such as buzzer, liquid crystal display shows the desired output.

Initially, Fingerprint verification is done by using the fingerprint sensor. The fingerprint sensor used is R307 fingerprint sensor. The block diagram of the system has been shown in Fig. 2.After the profitable verification of fingerprint, gadget will check with the data. Once it matches, then the server will check whether the voter has already casted vote or not. If the person already casted the vote, then the Buzzer will sound. If not casted vote then vote casting system lets in to cast his vote. Using the pushbutton voter can cast the vote. After successful voting, server will be updated.

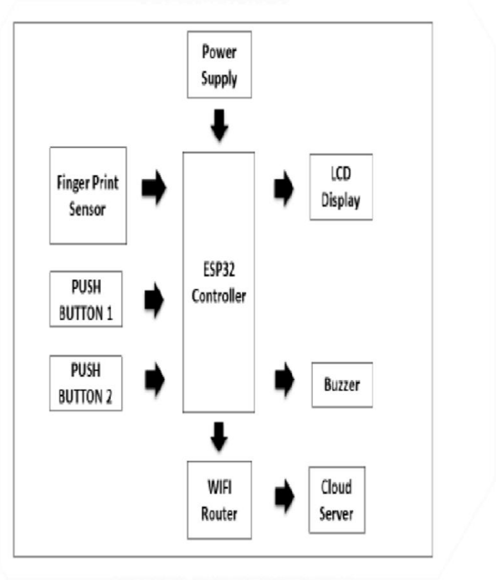


Figure 2: Block Diagram of the proposed system

We can additionally see the balloting counts in the "Blynk legacy" application. When final voter forged his vote, we have the vote casting counts equipped in server, election officer can announce the end result on the day of Election. So with the aid of the use of this system we can avoid the counting time of votes and man power. So, manual errors can be avoided which can occur while counting and also the malpractice will be in control.

V. Working Principle

The Fingerprint Sensor captures the Fingerprint of the voter. Then the pores and skin on the palms of our fingers has a one of a kind pattern called friction ridges that help us grab matters effectively barring slipping. These patterns consist of ridges and valleys arranged in positive configurations and are unique for every individual. When a finger comes in contact with a surface, the ridges make robust contact with it. These ridges are fed as input to ESP 32 Controller. In the ESP 32 Controller, the ADC converter which is an built in system, converts these ridges into digital layout i.e. 0s and 1s.

Then for each fingerprint an ID is created and personal details of the voter are fed using The Arduino Uno Software . This step is applied to avoid any confusions , then the converted fingerprint value and ID is stored .

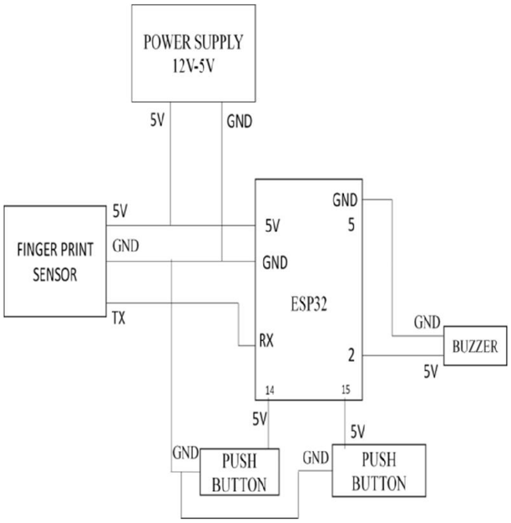


Figure 3: Circuit Diagram of proposed system

DOI: 10.48175/IJARSCT-3735

After the voter has voted, the liquid crystal display shows "Name Voted" and the party to which the candidate had solid their vote . When matching, the user places the finger and the device will generate a template of the finger and evaluate it with templates of the finger library. For 1:1 matching, the system will evaluate the live finger with a particular template designated in the Module; for 1: N matching, or searching, the gadget will search the total finger library for the matching finger.

If the voter tries once more to cast their vote , then the liquid crystal display shows the message as "Already Voted" then the crimson LED starts glowing and the Buzzer sound appears. Also the ESP 32 controller sends the details of the voters like "Name Voted" ,the non-public important points of the voter and balloting counts to the IoT Application via Arduino Uno Software. The IoT Application used here is “ Blynk Legacy Application”. This Application suggests the voting matter and the character who has voted.

VI. Result

After the implementation of the proposed system, The final output will be displayed as shown in below fig .This will be very efficient for the users to check the vote counts and whether his/her vote has been forged or not. The LCD output and stimulated output has been shown in below Fig .4 and Fig 5.And the final output of the application are also added in Fig 6.

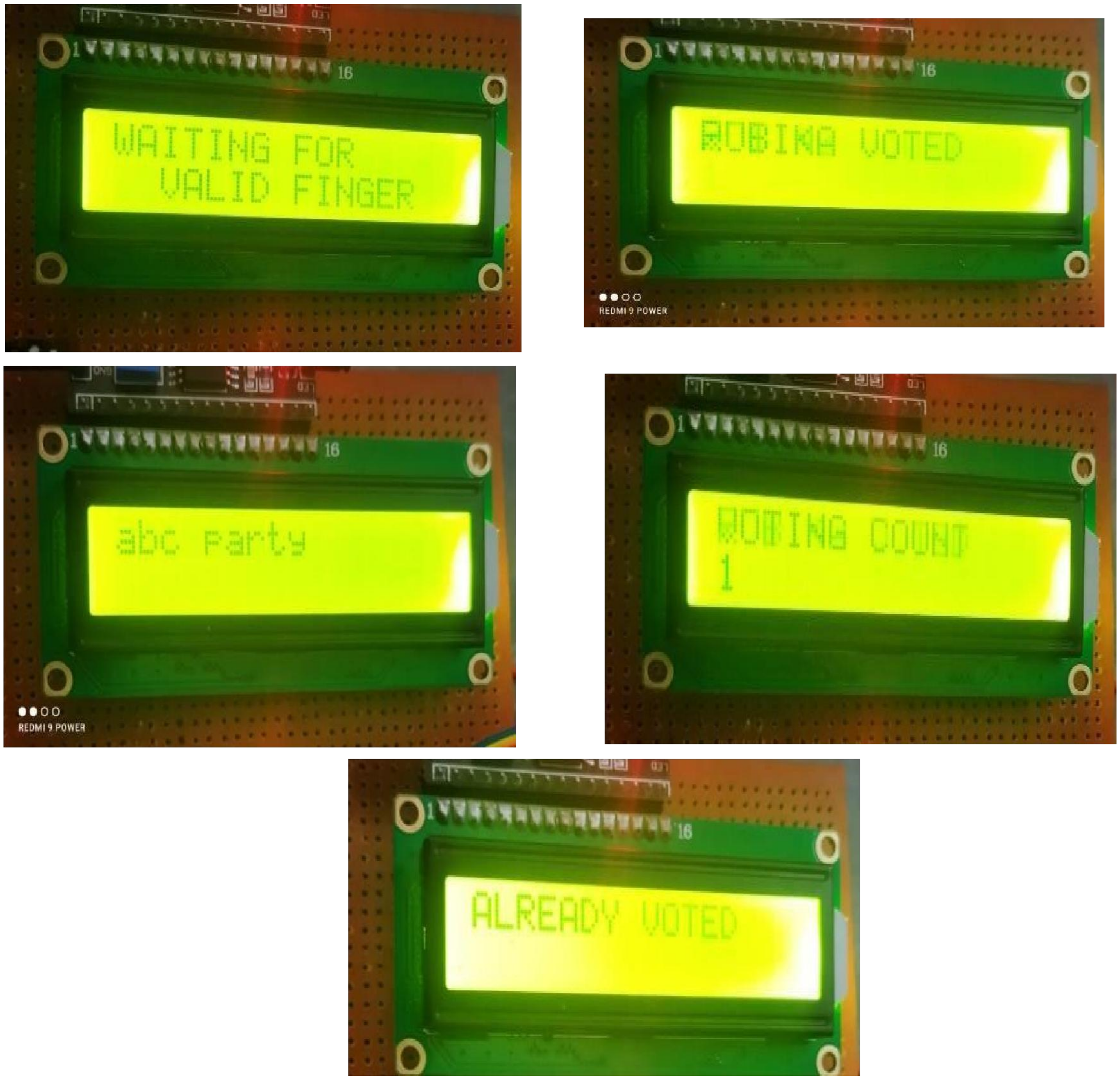
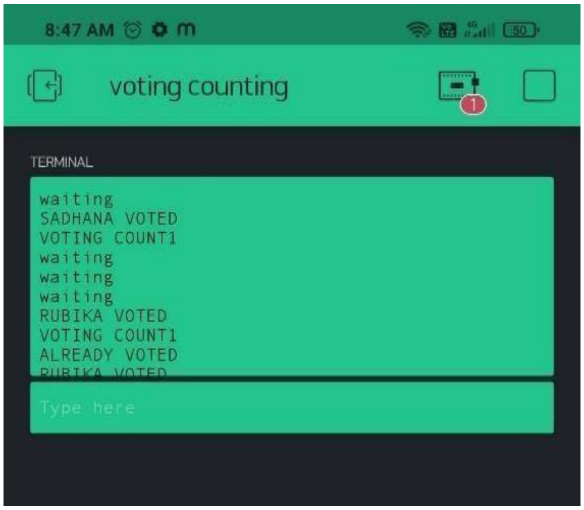


Figure 4: LCD Screen Output

Impact Factor: 6.252



```
waiting
SADHANA VOTED
VOTING COUNT1
waiting
waiting
waiting
RUBIKA VOTED
VOTING COUNT1
ALREADY VOTED
RUBIKA VOTED
```

Figure 5: Output from the Application

VII. Future Scope

In this system, we can add any other units for higher performance. Based on the work presented in this thesis, there are several number of advanced features that we can add to the system. Feature combinations in multimodal biometric can be worked upon through a number of mixtures of features. We should work on devising an algorithm which can predict the minutiae points, gender and the precise age of the individual to whom the fingerprint belongs.

VIII. Conclusion

In the existing paper, the system has been devised which overcomes most of the troubles confronted in the current vote casting system. This machine will ensure a more impenetrable voting technique surely, which is pretty required for the standard boom of a developing nation. The fingerprint primarily based voting gadget that has been proposed in this paper is faster and greater efficient than the systems mentioned in literature previously. Hence, it is recommended that the proposed device needs to be implemented at the national level, for getting the main advantage of making the e-voting system comprehensively.

References

[1]. A.Balamurali, Potru Sarada Sravanthi, B.Rupa, “Smart and secure voting machine using

[2]. biometrics,” 4th International Conference on Innovative system and control (ICICSC), 2020

[3]. S.Ganesh prabhu, R.R. Thirunavukarasu, Nizzarahammedd, Raghul., P. Jayarajan, “Smart Online Voting System,” 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021

[4]. Samarnath agarwal, Param dev, Afreen haider, Rajeevan chandel, “Biometric based secure remote electronic voting system,” IEEE 7th International Conference on Smart Structured and Systems (ICSSS), 2020

[5]. Sudeepthi komatenini, Gowtham lingala, “Secured E-Voting system using two factor biometric authentication,” 4th International Conference on Computing Methodologies and Communication (ICCMC), 2020

[6]. G.Rama lakshmi, V.Likhitha, K. V. Renuka, CH. Sri Rekha, T. Alekhya, “E-Voting system using biometrics,” International Conference on Intelligent Computing and Control Systems (ICICCS), 2019

[7]. A.M. Jagtap, V. Kesarkar and A. Supekar, “Electronic Voting System using Biometrics, Raspberry Pi and TFT module,” 3rd International Conference on Smart Trends in Electronics and Informatics (ICOEI), 2019

[8]. Sunita. Patil, Amish Bansal, U. Raina, V. Pujari and R. Kumar, “E-Smart Voting System with Secure Data Identification Using Cryptography,”3rd International Conference for Convergence in Technology (I2CT), 2018.

[9]. R. Govindaraj, P. Kumaresan and K. Sree harshitha, “Online Voting System using Cloud,” International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020

DOI: 10.48175/IJARSCT-3735