Value Embedded Quality Technical Education

A
SEMINAR REPORT
ON

SECURED AND TRANSPARENT VOTING SYSTEM USING BIO-METRICS

Third Year Computer Engineering

BY

Kalpesh Rane
Exam Seat No : T150694310
Roll No : 37

Under The Guidance of

Prof.R.S.Jagale

DEPARTMENT OF COMPUTER ENGINEERING

University of Pune
Gokhale Education Society's
R. H. Sapat College of Engineering,
Management Studies and Research,
Nashik - 422 005, (M.S.), INDIA

Gokhale Education Society's

R. H. Sapat College of Engineering, Management Studies and Research,

Nashik - 422 005, (M.S.), INDIA

CERTIFICATE

This is to certify that the seminar report entitled ***"SECURED AND TRANSPARENT VOTING SYSTEM USING BIOMETRICS"*** is being submitted herewith by "Kalpesh Bharat Rane, T150694310" has successfully completed his seminar work in partial fulfillment of requirements for the degree of Third Year Computer Engineering of Savitribai Phule Pune University.

Prof. Prof. R.S. Jagale	Dr. D.V. Patil
Seminar Guide	Head of the Department

Gokhale Education Society's

R. H. Sapat College of Engineering, Management Studies and Research,

Nashik - 422 005, (M.S.), INDIA

Seminar Approval Sheet

This Seminar entitled

"SECURED AND TRANSPARENT VOTING SYSTEM USING BIOMETRICS"

prepared and submitted by "Kalpesh Bharat Rane" has been approved and accepted in partial fulfillment of the requirements for the degree Third Year Computer Engineering.

Prof. R.S.Jagale	**Ms. R. D. Narwade**
Seminar Guide	**Seminar Coordinator**

Acknowledgement

I would like to express my sincere gratitude to everyone for providing their invaluable guidance, comments and suggestion throughout the course of seminar project. I would specially thank Prof R.S. Jagale for timely checking my progress constantly motivating me to work harder.

In this report, I hope to highlight the enormous opportunities presented by technology for making the election system of our country totally tamper proof and secure.in my desire to work this report I have in no way any claim to come out with a perfect piece of work.

These few details lead me to realize that like all human endeavors this project is not perfect and may contain errors and shortcomings. Thus I remain open to all criticisms and suggestions which could present me with new sources of inspiration as I develop my ability to research and learn.

Abstract

Every citizen or voter of India is allowed to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and/or to choose their government and political representatives through casting their votes. To allow the exercise of this right, almost all voting systems include the following steps: voter identification and authentication, voting and recording of votes cast, vote counting, publication of election results. Voter identification is required during electoral process. Security is a heart of e-voting process. Therefore, the necessity of designing a secure e-voting process is very important. A secured electronic voting machine using unique identification number i.e. AADHAR number has been developed. To provide additional security along with the AADHAR number biometric identification is used. At the time of voting in the elections, the voter authentication can be done through biometric pattern. If the biometric information of the voter matches the database of the AADHAR then the person is allowed to cast their vote. Transparency is additional advantage for the above system

Contents

List of Figures

List of Tables

Chapter 1

Introduction

As Abraham Lincoln famously quoted democracy as Democracy is for the people, by the people, of the people. Having an elected representative is the utmost feature of the democracy. Elections play a crucial part in choosing the capable leader which in-turn can impact the entire nation. As the largest democracy in the world, India has become a role model to other countries. Election Commission of India is the autonomous and statutory body which is responsible to conduct of free and fair elections. India is the largest democratic country in the world. Elections are conducted at various levels to choose their representatives by the people of the nation. The elections should be conducted in a right manner to ensure that the term Democracy should not lose its value. It is observed that there are so many problems associated with conduction of elections in the country such as percentage of voting is at most 60% in most of the cases, rigging in the elections etc. In Times of India (TOI) 24 Jan, 2009 11 lakhs fake voters in Delhi has found. Election commission has found 30000 illegal voters in the constituency of Sheila Dikshit. In total 1358179 voters have been found illegal in Delhi. In Bihar, Ram Vilas Paswan alleges 30% voter cards are identified as fake in Bihar.

1.1 SEMINAR IDEA

A Democracy is typically defined as a country where eligible citizens vote for their representatives, thus forming a Government for the people, by the people. The first general elections were held in the year 1951, with 173 million voters, and from there we have grown into a massive 725 million eligible voters by the year 2014 . India can be rightfully called the foremost epitome of Democracy. With such a large pool of voters, it is a difficult task to ensure that fair voting procedures are implemented at every polling booth in the country. The added fact that corrupt officials can be present at any polling booth, allowing malpractices and human errors in the process of voting is a concern.

1.2 MOTIVATION

The sole underlying purpose of a Democratic nation such as ours is to ensure that every citizen gets a fair chance to vote, without any mismanagement or anyone abusing their right to vote by employing dereliction. Such chances of human error can be eliminated by converting the whole election system into a standard tamper-

proof computerized system, which will leave no chance for errors or malpractice caused by human involvement. Fig.1 demonstrates the procedure for General Elections followed currently in India.

Chapter 2

LITRATURE REVIEW

2.1 Paper Surveys

1. **IEEE (ICISC 2018), Secured and transparent voting system using biometrics, Ch. Jaya Lakshmi, S. Kalpana [1]:-**

   This paper mainly focuses n solving all the election related problems on our country. This paper is very country specific as all the process is demonstrated and created by using EVM which is mainly used in our country.

   In this paper it is stated that every citizen or voter of India is allowed to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and/or to choose their government and political representatives through casting their votes. To allow the exercise of this right, almost all voting systems include the following steps: voter identification and authentication, voting and recording of votes cast, vote counting, publication of election results. Voter identification is required during electoral process. Security is a heart of e-voting process. Therefore, the necessity of designing a secure e-voting process is very important. A secured electronic voting machine using unique identification number i.e. AADHAR number has been developed. To provide additional security along with the AADHAR number biometric identification is used. At the time of voting in the elections, the voter authentication can be done through biometric pattern. If the biometric information of the voter matches the database of the AADHAR then the person is allowed to cast their vote. Transparency is additional advantage for the above system. This shows how much importance is given for solving the problem and also the researcher have included very less hardware related information in this paper.[1]

2. **RFID Based Biometric Voting Machine Linked to Aadhaar For Safe and Secure Voting, April 2015, International Journal of Science, Engineering and Technology Research (IJSETR)[3]:-**

   This paper was published in international journal of science, engineering and Technology. By the writers B. Madan Mohan Reddy, D. Srihari, this paper proposes a method for safe and secure Aadhaar based biometric voting system to avoid Aadhaar enrolment process is going on in Andhra Pradesh. At that time, Indian and every person persists in the database of Indian government. If Indian Government link this database to authors proposed method, Indian Government no need to collect details of finger print of every person. So, if

Indian Government adopt biometric voting system for voting purpose, we can easily avoid rigging in elections. One more authorized persons or constables who are in election duty. Because of Alcoholic sensor, we can provide peaceful environment at polling booth. If an unauthorized If already vote casted person enters into booth with his RFID tag for 2nd time voting, then also buzzer will alert booth level officer.[3]

This paper covers both the aspects i.e. Hardware components and software components.

3. ACM Conference on Computer and Communications Security (CCS 10), Oct. 2010, Security Analysis of Indias Electronic Voting Machines, Hari K. Prasad, J. Alex Halderman, Rop Gonggrijp Scott Wolchok, Eric Wustrow, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati [5]:-

   Elections in India are conducted almost exclusively using electronic voting machines developed over the past two decades by a pair of government-owned companies. These devices, known in India as EVMs, have been praised for their simple design, ease of use, and reliability, but recently they have also been criticized following widespread reports of election irregularities. Despite this criticism, many details of the machines design have never been publicly disclosed, and they have not been subjected to a rigorous, independent security evaluation. In this paper, a security analysis of a real Indian EVM obtained from an anonymous source. The machines design and operation in detail have been described, and its security in light of relevant election procedures Have been evaluated. Its concluded that in spite of the machines simplicity and minimal software trusted computing base, they are vulnerable to serious attacks that can alter election results and violate the secrecy of the ballot. The researchers demonstrate two attacks, implemented using custom hardware, which could be carried out by dishonest election insiders or other criminals with only brief physical access to the machines. This case study carries important lessons for Indian elections and for electronic voting security more generally.[5]

4. Fair Election System in India Using UID Data and Biometric Technology, Nikhil Shekhar Tilwani, Nivedita Majumdar, Pragati Bhargava, International Journal of Scientific Engineering Research, Volume 4, Issue 11, November-2013[6]:-

   India is the largest democratic country in the world, with an estimated 725 million eligible voters by the 2014 General Elections. With such a large population, the Election procedure is bound to be ridden with problems. The main issue here is fair elections. Every voting centre has a list of eligible voters from that constituency who can cast their vote. But it is common knowledge that there are a lot of centres, especially in semi-urban and rural areas where strict checking of voters id does not happen, as a result of which votes are cast on behalf of someone else, leading to unfair elections. The recent Unique Identification (UID) Aadhar system maintains a database of all residents of India along with their biometric data, which is unique to every citizen. This paper explores the concept of linking the biometric data in the UID database to the voting machine to ensure that every vote is cast by a person only once. Retrieval of data can be done and matched for every citizen with a UID. [6]

Chapter 3

Existing System

3.1 ELECTIONS (DEFINITION, TYPES AND HISTORY)

An election is a formal decision-making process by which a population or society chooses an individual to hold a political office. Elections have been the usual mechanism by which modern representative democracy operates that predates to as early as the 17th Century. Elections are conducted both by public entities such as the government as well as private and business organizations, for example, choosing representatives for the Board of directors of a company, professional club leadership and even, used in voluntary associations. In most democratic political systems, there are several types or categories of elections that are held which corresponds to the different layers of public governance or geographical jurisdiction. Common types of election categories thus include

- **Presidential Elections**
- **Parliamentary Elections**
- **Governorship Elections**
- **Local Government Elections**

3.2 VOTING PROCESS

To permit the exercise of this right, the majority voting systems around the world include the following steps: citizen identification and authentication, voting and recording of votes cast, vote counting, publication of election results.
Voter identification is needed during two phases of the electoral process: first for voter registration so as to determine the right to vote and subsequently, at voting time, to allow a citizen to exercise their right to vote by verifying if the person satisfies all the necessities required to vote (authentication). The election procedure dates back to ballot papers. Ballot papers had been used for almost 5-6 decades. In this paper based election voters cast their votes by simply depositing their ballots in sealed boxes distributed across the electoral centers around a given country. When the election period ends, all these boxes are opened and votes are counted manually in presence of the certified officials. In this process there can be error in counting of votes or in some cases voters find ways to vote more than

once. Sometimes votes are even manipulated to distort the results of an election in favor of certain candidates. With the advent of technology, ballot papers have been replaced by EVM (Electronic Voting Machine) to overcome drawbacks associated with ballot papers like stealing of ballot boxes, tearing of ballot papers, massive rigging, and physical damage to the ballot papers by pouring fluids etc.

3.3 ISSUES OF EXISTING VOTING SYSTEM

Electronic Voting Machines ("EVM"), Idea mooted by the Chief Election Commissioner in 1977. The EVMs were devised and designed by Election Commission of India in collaboration with Bharat Electronics Limited (BEL), Bangalore and Electronics Corporation of India Limited (ECIL), Hyderabad. The EVMs are now manufactured by the above two undertakings. An EVM consists of two units:

A) Control Unit **B) Balloting Unit**

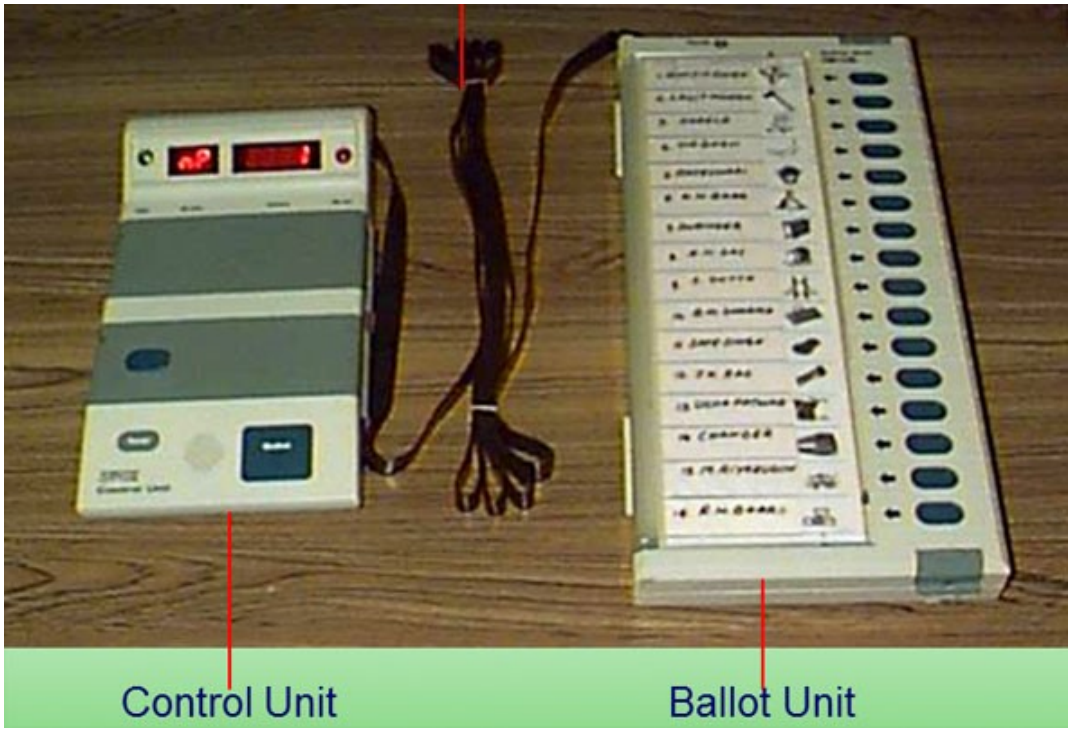

Figure 3.1: Interfacing of Control unit with Ballot Unit

There are many types of problems with EVM which is currently in use they are:

1. **Accuracy: It is not possible for a vote to be altered eliminated the invalid vote cannot be counted from the finally tally.**
2. **Democracy: It permits only eligible voters to vote and, it ensures that eligible voters vote only once.**
3. **Security Problems: One can change the program installed in the EVM and tamper the results after the polling. By replacing a small part of the machine with a look-alike component that can be silently instructed to steal a percentage of the votes in favour of a chosen candidate. These instructions can be sent wirelessly from a mobile phone**

4. **Illegal Voting (Rigging): The very commonly known problem Rigging which is faced in every electoral procedure. One candidate cast the votes of all the members or few amounts of members in the electoral list illegally. This results in the loss of votes for the other candidates participating and also increases the number votes to the candidate who performs this action. This can be done externally at the time of voting.**
5. **Privacy: Neither authority nor anyone else can link any ballot to the voter.**
6. **Verifiability: Independently verification of that all votes have been counted correctly.**

3.4 RELATED WORK

Direct Recording Electronic (DRE) voting system by S. Hashimi, S. Komatineni, and D. MacLean, it record votes by means of an electronic display provided with mechanical or electro-optical components that can be activated by the voter, that processes voter selections by means of a computer program, and that records that processed voting data in memory components.
Shafii Muhammad Abdulhamid et al developed an electronic voting system, which will solve manipulation of results to its barest minimum, this problem is mostly associated with the manual system of voting. The implementation of electronic voting system in Nigeria will boost the integrity of INEC and the result they produce. The programs used to develop this system are PHP, MySQL, Java Query, CSS and HTML.
Sahibzada Muhammad Ali et al proposed a Microcontroller Based Smart Electronic Voting Machine System which uses mechanical or electro-optical component like touch screen to provide ballot display. This machine was programmed to record voting data and then tabulates the voting data.
B. Madan Mohan Reddy et al proposed a method for voting purpose. One more advantage of this paper is, if an alcoholic person enters into polling booth, buzzer will alert authorized persons or constables who are in election duty. Because of Alcoholic sensor, we can provide peaceful environment at polling booth. If an unauthorized person enters into polling booth to cast his vote, buzzer will alert booth level officer. If already vote casted person enters into booth with his RFID tag for 2nd time voting, then also buzzer will alert booth level officer.

Chapter 4

PROPOSED VOTING SYSTEM

4.1 Authentication and Verification of the Voter

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In order to authenticate a person, we require them to have a valid Unique Identification (UID) number/Aadhar number. The number will be checked in the local database records first. If it is not found then it will search the central repository. It involves one-to-many match. If the persons number is not found in the central database then of course he/she will avoid of taking part in the voting process. On the other hand, if the number is present in the central database then the data of that person will be cached to the local database. This record is extracted from the local database and sent to authenticating servers for further processing.
For verification the persons fingerprint will be scanned at the client-side and matched one-to-one at the servers with the data extracted from the local database. This process puts less stress on the local database and improves data traffic. We use fingerprints for authentication because processing fingerprints is faster and better than other biometric data. Moreover, Aadhar details would be insufficient to establish the true identity of a person since they can be easily faked but by using fingerprints.
It is ensured that such fake entries are blocked right at the very beginning. In very situations, if the fingerprint identification is not working then the authentication of voter is verified through his/her iris pattern which is unique for every person

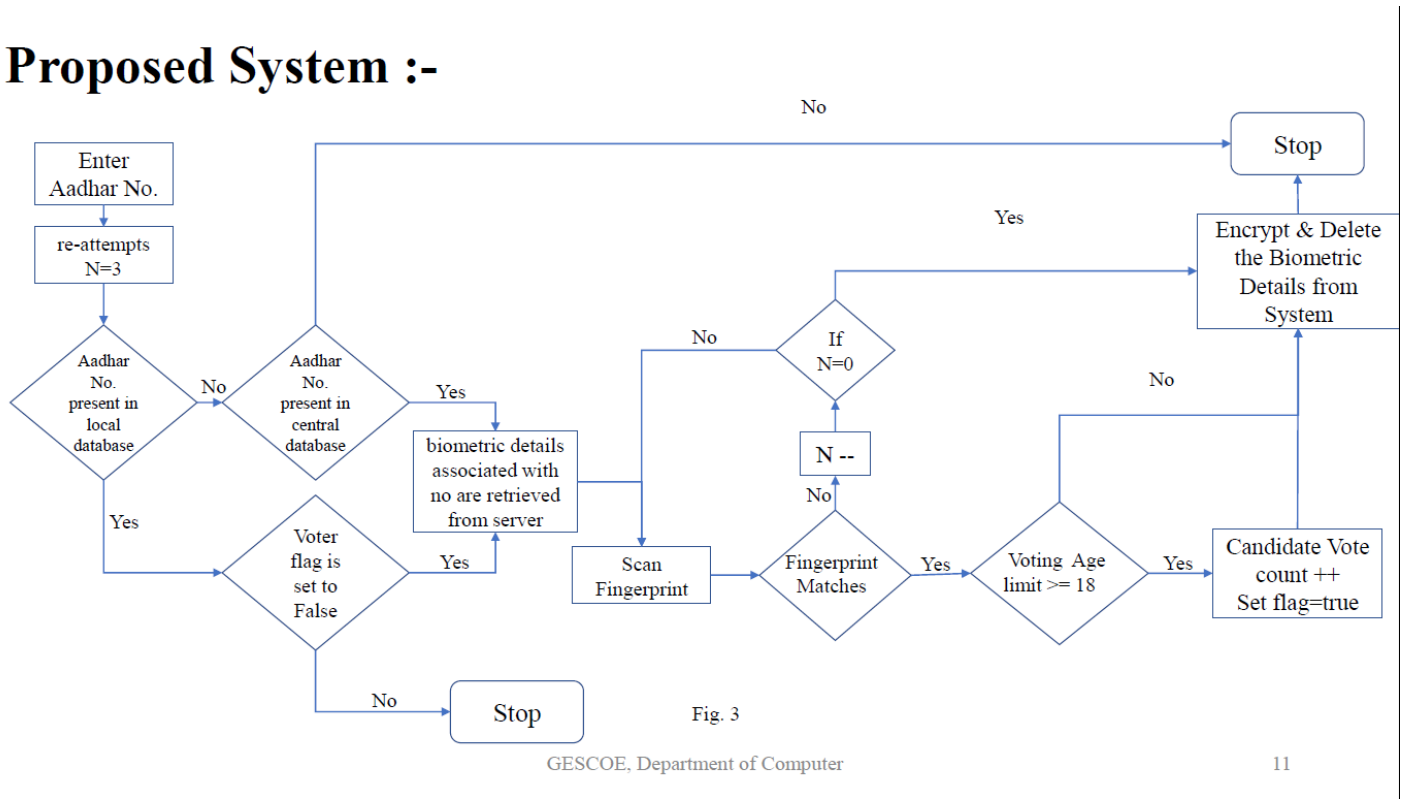

Figure 4.1: proposed system flowchart

4.2 PREVENTING FRAUDULENT VOTING

The first and the foremost thing to ensure proper voting is by accurately authenticating every voter. It is necessary to identify that every person coming to vote is unique otherwise it will violate the very principle of voting. Fingerprint matching ensures the authentication that the system requires. However, in order to improve accuracy, it is important to keep false reject rate (FRR) and false accept rate (FAR) as low as possible; practically close to zero. This can be achieved by using best finger method. Using 2 best fingers can improve the accuracy to 98% (FRR2%) with a single attempt and above 99 % (FRR 1%) with up to 3-attempts. Specifications of fingerprints and relevant details are provided in. To prevent underage individuals from voting, the system calculates persons age from the birth date present in the database records. If the calculated age is above permissible limit the person is allowed to vote and prevented otherwise. To prevent voters from voting two or multiple times we implement voting flags in the local databases. This flag is initially set to false. After the voter has cast the vote, his/her vote flag will be set to true. This will prevent the same person from voting again. These flags are temporary and can be reset after the election has completed so that the voter can participate in the next election.

4.3 GENERATING REPORTS

Whenever a voter casts a vote in favour of the candidate of choice, the vote count of that candidate gets incremented in the local database. The votes from all the local databases are summed up to get the final figure that the candidate has received. Thus this system provides instantaneous results and prevents unnecessary

use of manpower and wastage of time. Since this is an electronic system and uses digital data it has several advantages. Statistics can be generated from the obtained data for e.g. we could answer how many people have voted from a certain region, how many females voted, which age group voted the most, the highest turnouts, comparisons from previous years, etc. all that was not possible from traditional voting methods not even from EVMs. It would provide important insights into the election results and help improve the system even further

4.4 HARDWARE COMPONENTS

Figure 4.2: Fingerprint Sensor

4.4.1 Biometric Module

Firstly, discussing about Biometrics concentration comes on Fingerprint scanner. For this the R305 has high voltage module as a scanner. This module has in-built ROM, DSP and RAM. This can store up to 100 users fingerprint. This module can operate in 2 modes they are Master mode and User mode. The Master mode is used to register the fingerprints which will be stored in the ROM present on the scanner with a unique id. The R305 fingerprint sensor module is shown in the Fig.

- **PRINCIPLES OF OPERATION**

Fingerprint Sensor Type	Optical
Image Capture Surface	15-18(mm)
Static Indicator	15KV Backlight: Bright Red
Interface	USB1.1/UART (TTL Logical Level)
Dimension	55*32*21.5mm
Template Size	512 bytes
Verification Speed	03 Seconds
Scanning Speed	0.5 Seconds
Character File Size	256 Bytes

Table 4.1: Specifications of R305 fingerprint module

Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1: N). When enrolling, user needs to enter the finger two times. The system will process the two-time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1: N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

4.4.2 Arduino Uno

Arduino is open source physical processing which is based on a microcontroller board and an incorporated development environment for the board to be programmed. Arduino gains a few inputs, for example, switches or sensors and control a few multiple outputs, for example, lights, engine and others. Arduino program can run on Windows, Macintosh and Linux operating systems (OS) opposite to most microcontrollers frameworks which run only on Windows. Arduino programming is easy to learn and apply to beginners and amateurs. Arduino is an instrument used to build a better version of a computer which can control, interact and sense more than a normal desktop computer. It's an opensource physical processing stage focused around a straightforward microcontroller board, and an environment for composing programs for the board. Arduino can be utilized to create interactive items, taking inputs from a diverse collection of switches or sensors, and controlling an assortment of lights, engines, and other physical outputs.

4.4.3 Liquid Crystal Display (LCD):

A liquid crystal display (LCD) is a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector. Each pixel consists of a column of liquid crystal molecules suspended between two transparent electrodes, and two polarizing filters, the axes of polarity of which are perpendicular to each other. Without the liquid crystals between them, light

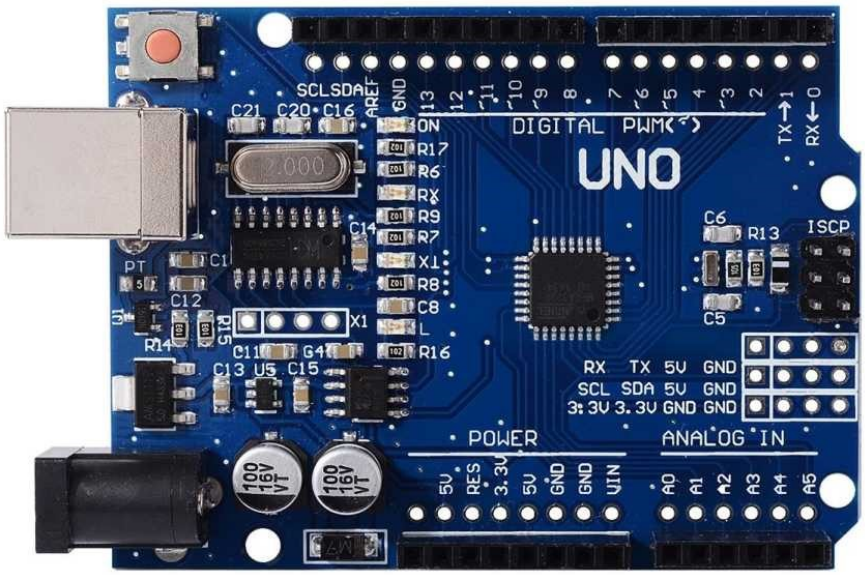

Figure 4.3: Arduino Uno Processor

passing through one would be blocked by the other. The liquid crystal twists the polarization of light entering one filter to allow it to pass through the other. A program must interact with the outside world using input and output devices that communicate directly with a human being. One of the most common devices attached to an controller is an LCD display. Some of the most common LCDs connected to the contollers are 16X1, 16x2 and 20x2 displays. This means 16 characters per line by 1 line 16 characters per line by 2 lines and 20 characters per line by 2 lines, respectively.

Figure 4.4: LCD Display

4.4.4 Arduino Uno

A very simple circuit to experiment with AT90S2313, 2x16 LCD display and 3x4 keypad. The clock based on 4 MHz crystal, but you can use anyone crystal between 1-4 MHz the keys with the name "A", "B", "F" is typed to the LCD with numbers 10-16. The circuit board consists of 7 digital I/O lines on a downstream 9-way D-type plug. This routes each bit to a particular line of the keypad. Columns 1, 2 and 3 and routed to bits 0, 1, and 2 respectively. Rows 1, 2, 3 and 4 and routed to bits 5, 6, 7 and 8 respectively. These values were chosen to enable the use of interrupts when connecting the keypad to Port B. The Matrix keypad is shown in the Fig 4.5

Figure 4.5: Matrix Keypad

1. **Features and Function**
   Essex Keypads are weather proof and extremely rugged. They use piezo-electric technology for sensing key depressions. Since there are no moving parts, the unit can withstand millions of keystrokes. Output from the unit is 26 Bit Wiegand and interfaces to Keri Systems' PXL-250W Tiger Controller (Wiegand capable). Red and green LEDs as well as a beeper provide user feedback to indicate if access is granted or denied. There is one jumper to set for keypad installation setting the operating voltage for the keypad (+5 VDC or +12 VDC). For complete instructions on working with an access control system, consult the PXL250 Tiger Controller Technical Reference that is shipped with the PXL-250.
2. **Specifications of Keypad is given below in Table 4.2**

Operating Environment	100% Relative Humidity
Operating Temperature	-40C to +70C (-40F to +160F)
Current Drawr	20A at 5VDC or 12 VDC

Table 4.2: Specifications of R305 fingerprint module

After uploading the program in Arduino Aadhar number is entered and fingerprint is asked to scan. When the fingerprint is registered an id of the person is produced in the serial port.

Chapter 5

RESULTS

1. **displays the welcome note for the voter. This welcome note alerts the voter and the voter is directed to follow the remaining steps in order.**
2. **displays the following note ENTER AADHAR NO therefore the voter is requested to give the UID number.**
3. **When the UID number is given by voter, then the number is verified in the Local Database and if it matches the voter is requested to give his/her biometric**
4. **Now the voter is requested to give the biometric and the given biometric is cross checked with the database which is stored. If both the fingerprint and the UID number matches then the age of the voter is verified and if he/she is eligible.**
5. **If the eligibility criteria is satisfied then the ballot is opened and the voter is allowed to cast his/her vote to a single party of his/her own choice**
6. **If the biometric and the UID number does not match with Local Database the not eligible is displayed,**

Chapter 6

CONCLUSION

6.1 CONCLUSION

The proposed voting system had many advantages over the traditional method of voting. This system affords additional security by allowing voter to vote only once by imparting unique identification along with biometric information. This system avoids fraudulent voting and illegal practices during the elections which is the key issue in the traditional voting system. This system provides transparency in the counting process. The advantages of this system are economic, faster tabulation of results, improved accessibility, greater accuracy, and lower risk of human and mechanical errors. Database consisting of the details like age, biometric of the people should be updated every time before election. Information about the casted vote can be sent to the voter through the messaging system.

6.2 Future Work:-

A biometric technique for authentication of voter can be said to be a solid system, because biometric authentication can never be wrong. But a problem may arise in management of such a large database. Secure Connections are needed for confidential data retrieval of the information. Not every citizen has been registered in the Aadhaar System and implementing the procedure will take a long time, owing to the fact that there are more than 700 million projected voters. Cost will also be high, as biometric authentication devices are very costly. Illiterate voters will definitely face a problem in using the machine. The system is tedious to implement, but once it is done, can be a very effective authentication procedure. With proper authentication and voter registration, fair elections can be ensured.

Chapter 7

References

[1] CH Jaya Lakshmi, S Kalpana (2018) ***VOTING SYSTEM USING BIOMETRICS*** for Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018)

[2] ***wikipedia***

[3] B. Madan Mohan Reddy, D. Srihari ***RFID Based Biometric Voting Machine Linked To Aadhaar For Safe And Secure Voting*** International Journal of Science, Engineering and Technology Research (IJSETR)

[4] ***(2012). Role of Biometric Technology in Aadhaar Authentication***

[5] Hari K. Prasad J. Alex Halderman Rop Gonggrijp Scott Wolchok Eric Wustrow Arun Kankipati Sai Krishna Sakhamuri Vasavya Yagat, ***Security Analysis of Indias Electronic Voting Machines***To appear in Proc. 17th ACM Conference on Computer and Communications Security (CCS 10), Oct. 2010

[6] Nikhil Shekhar Tilwani, Nivedita Majumdar, Pragati Bhargava ***Fair Election System in India Using UID Data and Biometric Technologyr*** International Journal of Scientific Engineering Research, Volume 4, Issue 11, November-2013