

ARDUINO BASED AUTHENTICATED VOTING MACHINE USING RFID AND FINGERPRINT FOR THE STUDENT ELECTIONS

Submitted in partial fulfillment of the
requirements for the award of
Bachelor of Technology degree in Information Technology

By

**RAJA GANESH .A (REG NO-39120090)
SAKTHI GANESH .S (REG NO - 39120099)**



**DEPARTMENT OF INFORMATION TECHNOLOGY
SCHOOL OF COMPUTING**

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC
JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI – 600119

APRIL – 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND
TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in

DEPARTMENT OF INFORMATION TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that this Final Year Project Report is the bonafide work of RAJA GANESH (REG NO: 39120090) AND SAKTHI GANESH (REG NO: 39120099) who have done the project work as an individual who carried out the project entitled "ARDUINO BASED AUTHENTICATED VOTING MACHINE USING RFID AND FINGERPRINT FOR STUDENT ELECTIONS" under my supervision from Jan 2023 to April 2023.

Internal Guide

DR.SENDURU SRINIVASULU , M.Tech. , Ph.D.

Head of the Department

DR.R.Subhashini , M.E., Ph.D.

Submitted for Viva voce Examination held on 11/05/2023

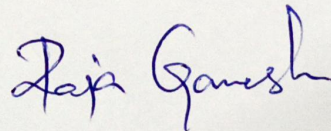
Internal Examiner

External Examiner

DECLARATION

I, Raja Ganesh (REG NO: 39120090), hereby declare that the Project Report on **"ARDUINO BASED AUTHENTICATED VOTING MACHINE USING RFID AND FINGERPRINT FOR STUDENT ELECTIONS"** done by us under the guidance of **Dr.Senduru Srinivasulu M.Tech.,Ph.D**, at Sathyabama Institute of Science and technology is submitted in partial fulfilment of the requirements of the award of Bachelor of Technology degree in Information Technology.

DATE: 10/05/23



PLACE: Chennai

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph. D, Dean**, School of Computing, **Dr.R.Subhashini, M.E., Ph.D**, Head of the Department of Information Technology for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.Senduru Srinivasulu M.Tech.,Ph.D**,for his valuable guidance, suggestions and constant encouragement paved the way for the successful completion of my phase-1 project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Information Technology** who were helpful in many ways for the completion of the project.

ABSTRACT

The guiding principles of democracy are free elections. Through elections, people reaffirm their voice, their beliefs, and select someone whose ideas support them most. Voters will elect their representatives via elections. The purpose of the elections is not only to decide the outcome but also to give the winners credence, also for those voters who did not bother to vote for them. The need to hold free, equal, and secret elections is emphasized here. It involves the supervision of elections by free, accountable, impartial and autonomous electoral bodies. As the phrase is 'today teens, tomorrow's citizens,' the student community needs the process of elections to be involved, trained, and acquainted with. Under this respect, the institutions of Higher education holds elections in the form of general elections to the office of the student councils. This student will receive first-hand information about filing nominations and scrutiny. of papers, withdrawing, canvassing, addressing, and most importantly, voting. The use of technology in voting will make it easier, more effective, and less prone to breaches of security. Technology will boost and speed up the safety of all votes and make the counting and automated verification much more effective. The design of an advanced voting system is a It is a difficult task as many main requirements have to be met. The secrecy of a poll should be maintained. No proof of which candidate gets a particular vote shall be provided by the voting system. The authors implemented the Authenticated Voting Machine in the elections described in this paper to ease the process and improve transparency. The concept is still in its infancy. It requires more research to keep it stable and theoretically strong. To ensure protection, the model uses radio frequency and fingerprint recognition and an IOT-based system.

TABLE OF CONTENTS

Chapter No	TITLE	Page No.
	ABSTRACT	v
	LIST OF FIGURES	vii
1	INTRODUCTION	1
2	LITERATURE SURVEY	2
	2.1 Inferences from Literature Survey	
	2.2 Open problems in Existing System	3
3	REQUIREMENTS ANALYSIS	4
	3.1 Feasibility Studies/Risk Analysis of the Project	4
	3.2 Hardware Requirements Specification Document	4
	3.3 Software Requirements Specification Document	4
4	DESCRIPTION OF PROPOSED SYSTEM	5
	4.1 Selected Methodology or process model	5
	4.2 Architecture / Overall Design of Proposed System	29
	4.3 Work Flow Method	30
5	IMPLEMENTATION DETAILS	31
	5.1 Development and Deployment Setup	31
	5.2 Testing	32
6	RESULTS AND DISCUSSION	33
7	CONCLUSION	34
	REFERENCES	35
	APPENDIX	
	A. SCREENSHOTS	38

LIST OF FIGURES

FIGURE NO	TITLE	PAGE NO
4.1.1	Arduino Uno	7
4.1.2	Pin configuration	9
4.1.3	RFID Chip	12
4.1.4	RFID Reader	13
4.1.5	Switch Pad	15
4.1.6	LCD Display	17
4.1.7	LCD laser diagram	18
4.1.8	Block diagram of power supply unit	22
4.1.9	Process of power supply unit	22
4.1.10	Arduino IDE Platform	25
4.2.1	Architecture diagram	29
4.2.2	Work Flow Diagram	30

CHAPTER 1

INTRODUCTION

Elections are an important feature of the democratic arrangement. To make the students understand the concepts of democratic structure and to install leadership qualities, elections are conducted. Technology has brought drastic changes in almost every field; the election process is not an exception to this. People rely on technology to make their work easy, fast, and accurate. The conventional paper ballot-based voting system is simple, but it is not transparent and error-free. We overcome the limitations of conventional paper-based ballots. An Authenticated Voting System (AVM) was introduced. It uses two levels of authentication, namely Radio Frequency Identification (RFID) and biometric. During the time of the admission process, the biometrics of every person are recorded and stored along with other necessary documents. Once the admission process is complete, RFID-based identity cards are issued to each one. This ID card is the first identity proof for the election. A student who possesses a valid ID card can only participate in the election process. During the election process, the voter places the RFID card on the card reader. The second level of authentication is used to ensure that the card belongs to the same person who possesses it. In the second level biometrics, the student is accepted using a fingerprint scanner available on the voting machine. This fingerprint is compared to that of the one stored in the database. If both the fingerprints match, then only that voter is permitted to vote. The necessary details are stored in the college database, and the votes are stored in the voting machine itself. The voting system under discussion works for a maximum of three candidates for a single post. If there are more posts, then a separate voting machine is to be used for each post. To speed up the voting process when there are thousands of students, the entire college is logically divided into several blocks, and the number of AVM units required is equal to the number of blocks, plus each of the blocks contains a booth-level operator (BLO). Fingerprint data of students will be retrieved for the college database. To do so, internet connectivity, preferably Wi-Fi, is needed. This paper outlines specifications for pre-implementation, system architecture, modular decomposition, user interfaces, device operation, and potential for development.

CHAPTER 2

LITERATURE SURVEY

2.1 INFERENCES FROM LITERATURE SURVEY

By updating EVMs for the purpose of ensuring a fair and transparent election process in regards to safety, verification, and reliability components., several authors have contributed to improving the current electoral system an electronic voting with biometric verification offline and hybrid EVMs solution has been suggested[1]. In order to create a more dependable system, it also suggests a hybrid EVMs solution that combines the advantages of both online and offline voting systems. The results of the experiments the authors conducted out to assess the performance of the suggested system demonstrated that it is a workable option for secure electronic voting .An online voting system that utilizes the Aadhar ID system has been proposed[3] the authors argue that this system would eliminate the need for physical voter registration and could prevent duplicate voting. An author argues[4] that biometric identification the issues such as voter impersonation can be avoided in their respective paper.

A voting system that utilizes wireless communication and authentication has been proposed[10] to ensure the security and accuracy of the voting process which includes a unique identification number for each voter and a wireless communication protocol to transmit votes to a central server. An analysis of an e-voting system to ensure its correctness and security has been proposed[8].The proposed system includes a formal specification in the Z notation and a formal analysis using the model checker tool, SMV. A software for biometric electronic voting system has been set up [11] in various regional networks at every polling station with the aim of ensuring a high degree of precision in authenticating voters. The author [12] proposes a novel voting system based on statement voting, which allows voters to express their views on a specific issue rather than simply voting for a candidate. This system is intended to increase voter engagement and improve voting accuracy. The current voting system has many issues, and it has been suggested that an external or internal attacker could change or tamper with the date bases[13]. This paper[14] presents a blockchain-based electronic voting recording system design that employs smart contracts to ensure voting process integrity. The

author [16]reports on the use of blockchain technology for election voting in the United States. The system is intended to provide a secure, transparent, and real-time voting process. The authors discuss the importance of a secure and reliable voting system, particularly in democratic elections[17]. They also emphasise the potential advantages of an internet-based voting system, such as increased voter convenience and accessibility. They do, however, acknowledge the various security concerns that come with such a system, such as the possibility of fraud, hacking, and voter coercion. Voting transactions that keep track of the vote balances can be used to create a blockchain. Everyone can agree on the actual number because they can tally up the votes separately, and they can verify that no votes have been changed, deleted, or added illegally thanks to Blockchain's audit trail [18]. The authors begin by discussing the importance of electronic voting machines in modern elections and the advantages they have over traditional paper-based voting systems. They then examine the architecture of existing EVMs, highlighting the advantages and disadvantages of each approach. [19] The authors suggest a new EVM design based on a microcontroller and a touchscreen display. They go over the system's various components, such as the display, keypad, and communication interfaces. From theory to practise, a comprehensive overview of end-to-end verifiability in voting systems. [20] End-to-end verifiability, the authors argue, is required to ensure the integrity of the voting process, and they propose several methods for achieving this goal. This paper proposes[21] an electronic voting machine that identifies voters using the Aadhaar biometric system. The system is controlled by an Arduino microcontroller and can be easily deployed in remote locations.

2.2.OPEN PROBLEMS IN EXISTING SYSTEM:

While smart voting systems are becoming more and more popular as technology continues to advance, many fail to provide the user with a device. Many voting systems do not provide smart electronic security systems. standard, which is problematic due to the high rate of fraud. By using bio metric authentication systems, we can solve many of the problems that come with security systems and increase the efficiency of security systems.

Disadvantage:

- Here we only have bio metric, and buzzer alert systems
- We did not use OTP and password method.

CHAPTER 3

REQUIREMENT ANALYSIS

3.1.FEASIBILITY STUDIES/RISK ANALYSIS OF THE PROJECT

1. Security risks: There is a risk of the system being hacked or tampered with. It is important to ensure that the system is secure and protected from unauthorized access.
2. Technical risks: The system may encounter technical glitches, such as software errors, connectivity issues or hardware malfunction. Regular maintenance and testing is essential to prevent such issues.
3. User risks: There is a risk of user error, such as misplacement or damage of RFID tags, or failure to properly scan the fingerprint. Proper training and education of the users is important to prevent such risks.
4. Legal risks: There is a risk of the system not complying with the electoral laws of the country or region where it is being used. It is important to ensure that the system meets all the legal requirements and is approved by the relevant authorities.

Three key considerations involved in the feasibility analysis are

- Economical feasibility
- Technical feasibility
- Social feasibility

3.2.HARDWARE REQUIREMENTS SPECIFICATION DOCUMENT:

- Arduino
- Power supply unit
- Biometric scanner
- 4*3 KEYPAD
- GSM
- RFID
- LCD

3.3.SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT:

- Arduino IDE.
- Embedded C.

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

- It uses two levels of authentication namely Radio Frequency Identification (RFID) and biometric. During the time of the admission process, the biometric of every voters is recorded and stored along with other necessary documents. Once the admission process is complete RFID-based identity cards are issued to every voters. This ID card is the first identity proof for the election.
- The one who possesses a valid ID card can only participate in the election process. During the election process, the student places the RFID card on the card reader.
- To ensure that the card belongs to the same voter who possesses it, the second level of authentication is used. In the second level biometric of the student is accepted using a fingerprint scanner available on the voting machine.
- This fingerprint is compared to that of the one stored in the database. If both the match then PIN has to be entered. if entered PIN is correct then only the voters is permitted to vote.

4.1.SELECTED METHODOLOGY OR PROCESS MODEL:

4.1.1 ARDUINO UNO:

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. Revision 2 of the Uno board has a resistor pulling the 8U2 HWB line to ground, making it easier to put into DFU mode. Revision 3 of the board has the following new features:

- 1.0 pinout: added SDA and SCL pins that are near to the AREF pin and two other new pins placed near to the RESET pin, the IOREF that allow the shields to adapt to the voltage provided from the board. In future, shields will be compatible both with the board that use the AVR, which operate with 5V and with the Arduino Due that operate with 3.3V. The second one is a not connected pin, that is reserved for future purposes.

- Stronger RESET circuit.

- Atmega 16U2 replace the 8U2. "Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward. The Uno is the latest in a series of USB Arduino boards, and the reference model for the Arduino platform; for a comparison with previous versions, see the index of Arduino boards.

POWER:

The input voltage to the Arduino board when it's using an external power source (as opposed to 5 volts from the USB connection or other regulated power source). You can supply voltage through this pin, or, if supplying voltage via the power jack, access it through this pin.

- 5V. This pin outputs a regulated 5V from the regulator on the board. The board can be supplied with power either from the DC power jack (7 - 12V), the USB connector (5V), or the VIN pin of the board (7-12V). Supplying voltage via the 5V or 3.3V pins bypasses the regulator, and can damage your board. We don't advise it.

- 3V 3. A 3.3-volt supply generated by the on-board regulator. Maximum current draw is 50 mA.

- GND. Ground pins.

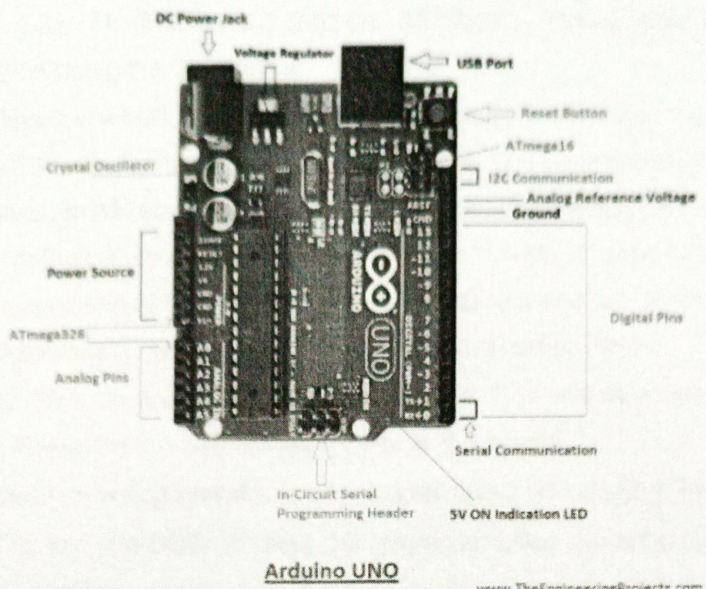


Figure 4.1.1 Arduino Uno

Memory

The ATmega328 has 32 KB (with 0.5 KB used for the bootloader). It also has 2 KB of SRAM and 1 KB of EEPROM (which can be read and written with the EEPROM library). Input and Output Each of the 14 digital pins on the Uno can be used as an input or output, using pin Mode(), digital Write(), and digital Read() functions. They operate at 5 volts. Each pin can provide or receive a maximum of 40 mA and has an internal pull-up resistor (disconnected by default) of 20-50 kilo Ohms.

In addition, some pins have specialized functions:

- **Serial:** 0 (RX) and 1 (TX). Used to receive (RX) and transmit (TX) TTL serial data. These pins are connected to the corresponding pins of the ATmega8U2 USB-to-TTL Serial chip.
- **External Interrupts:** 2 and 3. These pins can be configured to trigger an interrupt on a low value, a rising or falling edge, or a change in value. See the attach Interrupt () function for details.
- **PWM:** 3, 5, 6, 9, 10, and 11. Provide 8-bit PWM output with the analog Write () function.

- SPI: 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK). These pins support SPI communication using the SPI library.
- LED: 13. There is a built-in LED connected to digital pin 13. When the pin is HIGH value, the LED is on, when the pin is LOW, it's off. The Uno has 6 analog inputs, labeled A0 through A5, each of which provide 10 bits of resolution (i.e. 1024 different values). By default, they measure from ground to 5 volts, though is it possible to change the upper end of their range using the AREF pin and the analog Reference () function. Additionally, some pins have specialized functionality:
- TWI: A4 or SDA pin and A5 or SCL pin. Support TWI communication using the Wire library. There are a couple of other pins on the board:
- AREF. Reference voltage for the analog inputs. Used with analog Reference ().
- Reset. Bring this line LOW to reset the microcontroller. Typically used to add a reset button to shields which block the one on the board. See also the mapping between Arduino pins and ATmega328 ports. The mapping for the Atmega8, 168, and 328 is identical. Communication The Arduino Uno has a number of facilities for communicating with a computer, another Arduino, or other microcontrollers.

The ATmega328 provides UART TTL (5V) serial communication, which is available on digital pins 0 (RX) and 1 (TX). An ATmega16U2 on the board channels this serial communication over USB and appears as a virtual com port to software on the computer. The '16U2 firmware uses the standard USB COM drivers, and no external driver is needed.

However, on Windows, a .inf file is required. The Arduino software includes a serial monitor which allows simple textual data to be sent to and from the Arduino board. The RX and TX LEDs on the board will flash when data is being transmitted via the USB-to-serial chip and USB connection to the computer (but not for serial communication on pins 0 and 1). A Software Serial library allows for serial communication on any of the Uno's digital pins. The ATmega328 also supports I2C (TWI) and SPI communication. The Arduino software includes a Wire library to simplify use of the I2C bus; see the documentation for details. For SPI communication, use the SPI library.

PIN CONFIGURATION:

THE ARDUINO

MCU : Atmega 328
 Input voltage : 7V-12V
 Operating voltage : 5V
 CPU Speed : 16MHz
 Analog In/Out : 6/0
 Digital IO/PWM : 14/6
 EEPROM : 1KB
 SRAM : 2KB
 Flash : 32KB
 UART : 1
 USB : Regular

Sensor's Power - 200 mA Max

Analog In -

Access with analogRead(pin#)

returns mapped 0-5V to int 0-1023

Digital In/Out -

Set pin with pinMode(pin#, INPUT/OUTPUT)

OUTPUT - 40 mA Max

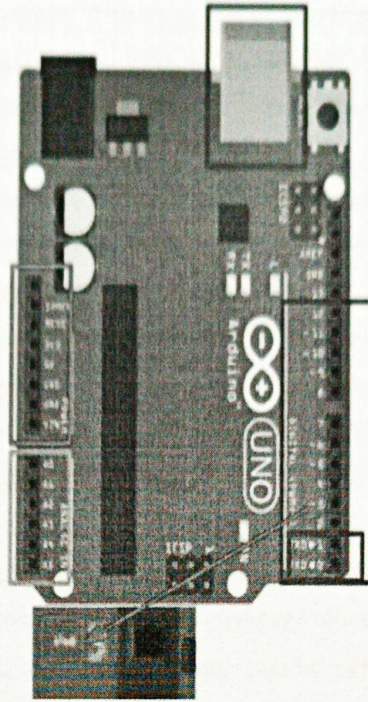
INPUT - return HIGH if > 3V else LOW

PWM (Pulse Width Modulated) signal

Access with analogWrite(pin#, Value)

0 < Value < 255 maps to 0 - 100% Duty cycle

Serial Communication Access Points



ARDUINO PIN	MICROCONTROLLER PIN
0	- PD0(RXD)
1	- PD1(TXD)
2	- PD2(INT0)
3	- PD3(INT1)
4	- PD4
5	- PD5
6	- PD6
7	- PD7
8	- PB0
9	- PB1
10	- PB2(SS)
11	- PB3(MOSI)
12	- PB4(MISO)
13	- PB5(SCK)
A0	- PC0
A1	- PC1
A2	- PC2
A3	- PC3
A4	- PC4(SDA)
A5	- PC5(SCL)

Pin out from: <http://arduino.cc/en/arduino-boards-pin-mapping/11>

Figure 4.1.2 Pin configuration

4.1.2 FINGER PRINT SENSOR:

Fingerprint scanners are security systems of biometrics. They are used to unlock doors and in other security applications. During the 2010s fingerprint scanners became commonplace on mobile phones.

TYPES

Optical reflexive

They are based on the oldest technique, that consists of placing your finger on a glass surface or a prism that is illuminated by a led diode. When the ridges of fingerprints touch the surface, the light is absorbed, while between these crests a total reflection occurs. The resulting light and dark areas are recorded in an image sensor. In practice there are some difficulties with this technique: the images obtained with wet and dry fingers are very different and, in addition, the system is sensitive to dust and dirt on the surface. The unit has a considerable size,

impractical and expensive. This system is easy to cheat and if the skin is damaged, the fingerprint is not recognized correctly. The recognition of the fingerprint of older people is also difficult to do because the skin is not elastic enough. In some circumstances this may result in false recognition. If the stored fingerprint was taken with less pressure, false acceptances may occur.

Capacitive The sensor is a silicon integrated circuit with a surface that is covered by a large number of transducer elements (or pixels), with a typical resolution of 500 dpi. Each element contains two adjacent metal electrodes. The capacity between the electrodes, which forms a feedback path for an inverting amplifier, is reduced when the finger is applied to said surface: it is further reduced when it detects ridges and less reduced when it detects the space between them. The sensor is susceptible to electrostatic discharge. These sensors only work with normal healthy skins, they are not operative being used on skins with hard areas, calluses or scars.

Moisture, grease or dust can also affect its operation. **Mechanical** It consists of tens of thousands of tiny pressure transducers that are mounted on the surface of the sensor. An alternative design uses switches that are closed when pressed by a ridge, but that stay open when they are under a valley. This only provides one bit of information per pixel, instead of working with a gray scale. **Thermal** In this case the heat driven by the finger is detected, which is greater when there is a ridge than when there is a valley. A silicon component has been developed with a matrix of pixels called Finger Chip; that is, finger integrated circuit, each of which is covered with a layer of pyroelectric material in which a change in temperature translates into a change in the load distribution of its surface.

The image is in the gray scale that has the right quality even with the finger worn, with dirt, with grease or with humidity. The sensor has a robust protective layer and can provide a dynamic output. **Dynamic output** Most of the sensors described have been altered in the past. To avoid this, a new operating mode has been added. Instead of simply placing your finger statically on the sensor, the finger moves slowly along it. The sensor only has a narrow sensitive area, and generates a complete sequence of images, which can be reassembled, by means of a processor, in a complete image. The benefits are improved appreciably and the elimination of any residual grease is guaranteed. **Uses** The most important use area is in access control for computers. This is especially important for laptops and PDAs. Thanks to the price falling, more and more devices are equipped with sensors. Other devices

with built-in fingerprint sensors include USB hard drives, USB memory modules and card readers. They are also available in mice and keyboards. Sensors are increasingly used to secure financial transactions and change machines for online banking. In the future, the owner's fingerprint will be stored securely on identity cards and credit cards and may also be used for authentication of emails using digital signatures. Direct physical access to rooms and devices can also be ensured by coupling fingerprint sensors with door opening systems.

4.1.3RFID:

RFID is an acronym for "radio-frequency identification" and refers to a technology whereby digital data encoded in RFID tags or smart labels (defined below) are captured by a reader via radio waves. RFID is similar to barcoding in that data from a tag or label are captured by a device that stores the data in a database. RFID, however, has several advantages over systems that use barcode asset tracking software. The most notable is that RFID tag data can be read outside the line-of-sight, whereas barcodes must be aligned with an optical scanner.

4.1.3.1 Working

RFID belongs to a group of technologies referred to as Automatic Identification and Data Capture (AIDC). AIDC methods automatically identify objects, collect data about them, and enter those data directly into computer systems with little or no human intervention. RFID methods utilize radio waves to accomplish this. At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader (also called an interrogator). The reader then converts the radio waves to a more usable form of data. Information collected from the tags is then transferred through a communications interface to a host computer system, where the data can be stored in a database and analyzed at a later time.

4.1.3.2. Defining RFID:

RFID or Radio Frequency Identification System is a technology-based identification system which helps identifying objects just through the tags attached to them, without requiring any light of sight between the tags and the tag reader. All that is needed is radio communication between the tag and the reader.

A Basic RFID System:

3 Main Components of a RFID System

- **A RFID tag:** It consists of a silicon microchip attached to a small antenna and mounted on a substrate and encapsulated in different materials like plastic or glass veil and with an adhesive on the back side to be attached to objects.

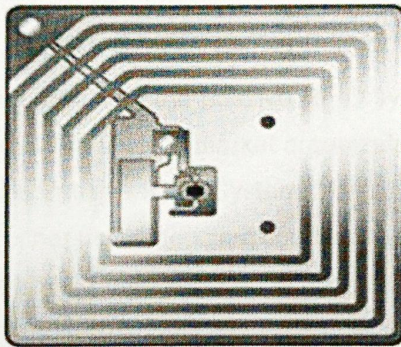


Figure 4.1.3 RFID Chip

RFID Tag

- **A reader:** It consists of a scanner with antennas to transmit and receive signals and is responsible for communication with the tag and receives the information from the tag.
- **A Processor or a Controller:** It can be a host computer with a Microprocessor or a microcontroller which receives the reader input and process the data.

2 Types of RFID Systems:

- **Active RFID system:** These are systems where the tag has its own power source like any external power supply unit or a battery. The only constraint being the life time of the power devices. These systems can be used for larger distances and to track high value goods like vehicles.

- **Passive RFID system:** These are systems where the tag gets power through the transfer of power from a reader antenna to the tag antenna. They are used for short range transmission.

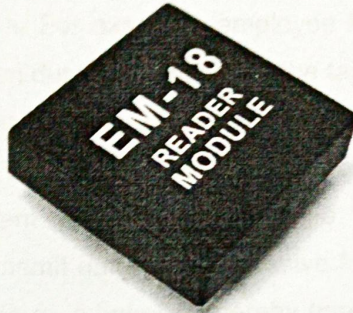


Figure 4.1.4 RFID Tag Reader

Here we are mostly concerned with the passive RFID system as it is most widely used in regular applications like in retail market organizations.

A brief idea about How the Passive RFID System Works:

The tag can be powered either using inducting coupling method or through EM wave capture method. Let's us have a brief knowledge about the system using these two methods.

A Passive RFID system using Induction coupling method: In this approach the RFID tag gets power from the reader through inductive coupling method. The reader consists of a coil connected to an AC supply such that a magnetic field is formed around it. The tag coil is placed in the vicinity of the reader coil and an electromotive force is induced it by the virtue of Faraday's law of induction. The EMF causes a flow of current in the coil, thus producing a magnetic field around it. By the virtue of Lenz law, the magnetic field of the tag coil opposes the reader's magnetic field and there will be a subsequent increase in the current through the reader coil. The reader intercepts this as the load information. This system is suitable for very short distance communication. The AC voltage appearing across the tag coil is converted to DC using rectifier and filter arrangement.

4.1.3.3. *RFID Tags and Smart Labels*

As stated above, an RFID tag consists of an integrated circuit and an antenna. The tag is also composed of a protective material that holds the pieces together and shields them from various environmental conditions. The protective material depends on the application. For example, employee ID badges containing RFID tags are typically made from durable plastic, and the tag is embedded between the layers of plastic. RFID tags come in a variety of shapes and sizes and are either passive or active. Passive tags are the most widely used, as they are smaller and less expensive to implement. Passive tags must be “powered up” by the RFID reader before they can transmit data. Unlike passive tags, active RFID tags have an onboard power supply (e.g., a battery), thereby enabling them to transmit data at all times.

Smart labels differ from RFID tags in that they incorporate both RFID and barcode technologies. They’re made of an adhesive label embedded with an RFID tag inlay, and they may also feature a barcode and/or other printed information. Smart labels can be encoded and printed on-demand using desktop label printers, whereas programming RFID tags are more time consuming and requires more advanced equipment.

4.1.3.4. *RFID Applications*

Although RFID technology has been in use since World War II, the demand for RFID equipment is increasing rapidly, in part due to mandates issued by the U.S. Department of Defense (DoD) and Wal-Mart requiring their suppliers to enable products to be traceable by RFID.

Whether or not RFID compliance is required, applications that currently use barcode technology are good candidates for upgrading to a system that uses RFID or some combination of the two. RFID offers many advantages over the barcode, particularly the fact that an RFID tag can hold much more data about an item than a barcode can. In addition, RFID tags are not susceptible to the damages that may be incurred by barcode labels, like ripping and smearing.

From the read distance to the types of tags available, RFID has come a long way since World War II and there is a bright future ahead.

4.1.4. 4X4 MEMBRANE SWITCH KEYPAD

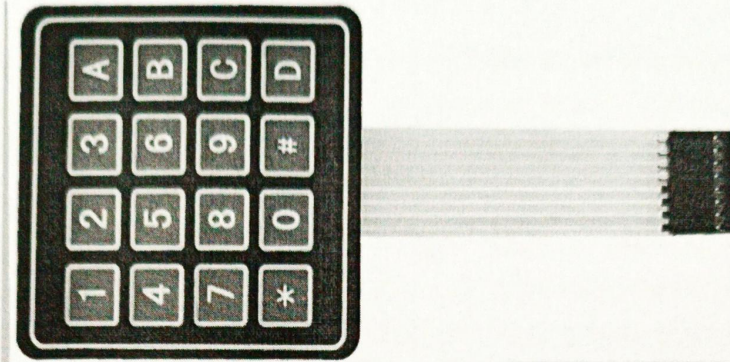


Figure 4.1.5 Switch Pad

Matrix Keyboard is a kind of keyboard whose layout is like a matrix and it's used as a peripheral equipment of MCU. The structure of matrix keyboard is more complex than that of other common keyboards, and the condition is similar to that of the recognition. The column line is connected with the anode of the power supply through resistors and let the I/O port of MCU connected with the row line work as an output terminal. The I/O port connected with the column line will be the input.

Because during the circuit design, there is much more need of external input. It will consume much IO source if we control a button separately, we have the matrix keyboard. The most common types are 4*4 and 8*8. Among them, the type 4*4 is even more common than 8*8.

On a keyboard, if there are too many buttons, we will arrange them into the form of matrix to decrease the using of the I/O port. In the internal structure of the matrix keyboard, each horizontal line and each vertical line are not connected directly at the intersection, but at the button. Therefore, a port (eg. P1) can form $4*4=16$ buttons, and the number is twice as much as that of the button whose port cable is connected with keyboard.

The larger the number of the wires, the clearer the difference. For example, if there is an additional wire, we can get a keyboard with 20 buttons; using the port cable

directly, we can get one additional key (key 9). So if there is much need of buttons, it is wise to use matrix analysis.

Membrane keypad is an application case of membrane switch with arrayed buttons. Membrane keypad is a kind of currently widespread operation system in the world that has the advantages of both practicality and beauty. It is composed of panel, upper circuit, isolation layer and bottom circuit. Due to these advantages: nice appearance, modern design, tiny in size, light weight, strong sealing (moisture proof, dust proof, oil pollution prevention, acid and alkali resistance), quake resistance and long service life, etc., it is commonly used in these fields, like medical instrument, computer control, digital machine tool, electronic weighing device, post and telecommunication, photocopier, refrigerator, microwave oven, electric fan, washing machine, electronic gaming machines.

4.1.5.LCD:

A liquid-crystal display (LCD) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in color or monochrome. LCDs are available to display arbitrary images (as in a general-purpose computer display) or fixed images with low information content, which can be displayed or hidden, such as preset words, digits, and seven-segment displays, as in a digital clock.

4.1.5.1.LCD Display:

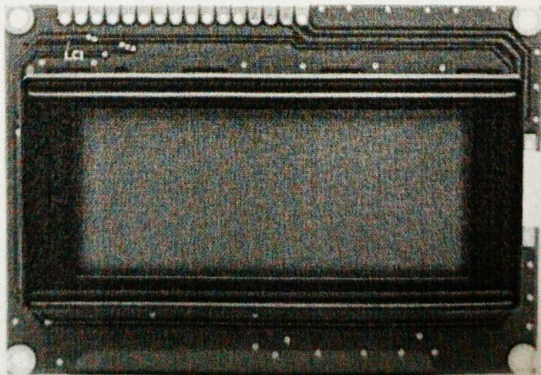


Figure 4.1.6 LCD Display

They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements. LCDs can either be normally on (positive) or off (negative), depending on the polarizer arrangement. For example, a character positive LCD with a backlight will have black lettering on a background that is the color of the backlight, and a character negative LCD will have a black background with the letters being of the same color as the backlight. Optical filters are added to white on blue LCDs to give them their characteristic appearance.

4.1.5.2. Working

The principle behind the LCD's is that when an electrical current is applied to the liquid crystal molecule, the molecule tends to untwist. This causes the angle of light which is passing through the molecule of the polarized glass and also cause a change in the angle of the top polarizing filter. As a result, a little light is allowed to pass the polarized glass through a particular area of the LCD. Thus, that particular area will become dark compared to other. The LCD works on the principle of blocking light. While constructing the LCD's, a reflected mirror is arranged at the back. An electrode plane is made of indium-tin oxide which is kept on top and a polarized glass with a polarizing film is also added on the bottom of the device. The complete region of the LCD has to be enclosed by a common electrode and above it should be the liquid crystal matter.

4.1.5.3. LCD Layer Diagram:

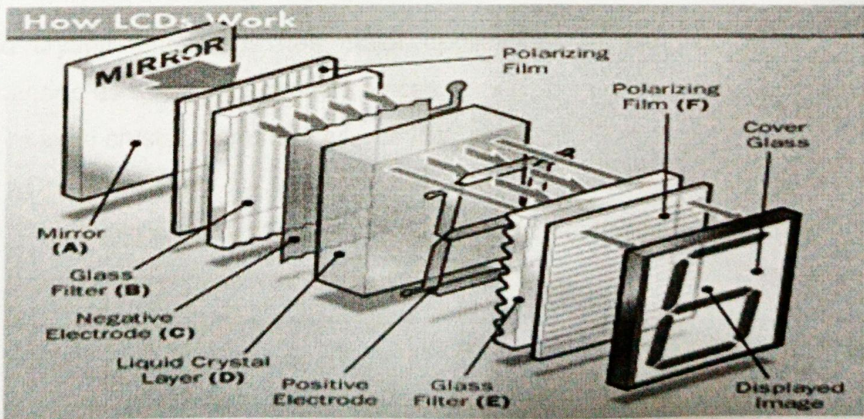


Figure 4.1.7 LCD Layer Diagram

Next comes to the second piece of glass with an electrode in the form of the rectangle on the bottom and, on top, another polarizing film. It must be considered that both the pieces are kept at right angles. When there is no current, the light passes through the front of the LCD it will be reflected by the mirror and bounced back. As the electrode is connected to a battery the current from it will cause the liquid crystals between the common-plane electrode and the electrode shaped like a rectangle to untwist. Thus, the light is blocked from passing through. That particular rectangular area appears blank.

4.1.5.4. Advantages of an LCD's:

- LCD consumes less amount of power compared to CRT and LED
- LCD are consisting of some microwatts for display in comparison to some mill watts for LED's
- LCD are of low cost
- Provides excellent contrast
- LCD are thinner and lighter when compared to cathode ray tube and LED.

4.1.5.5. Applications of Liquid Crystal Display

Liquid crystal technology has major applications in the field of science and engineering as well on electronic devices.

- Liquid crystal thermometer
- Optical imaging
- The liquid crystal display technique is also applicable in visualization of the radio frequency waves in the waveguide
- Used in the medical applications

4.1.6 GSM:

GSM (Global System for Mobile communications) is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices such as tablets. It was first deployed in Finland in December 1991.[2] As of 2014, it has become the global standard for mobile communications – with over 90% market share, operating in over 193 countries and territories.[3]

2G networks developed as a replacement for first generation (1G) analog cellular networks, and the GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony. This expanded over time to include data communications, first by circuit-switched transport, then by packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution, or EGPRS).

Network structure

The network is structured into a number of discrete sections:

- Base station subsystem – the base stations and their controllers
- Network and Switching Subsystem – the part of the network most similar to a fixed network, sometimes just called the "core network"
- GPRS Core Network – the optional part which allows packet-based Internet connections
- Operations support system (OSS) – network maintenance

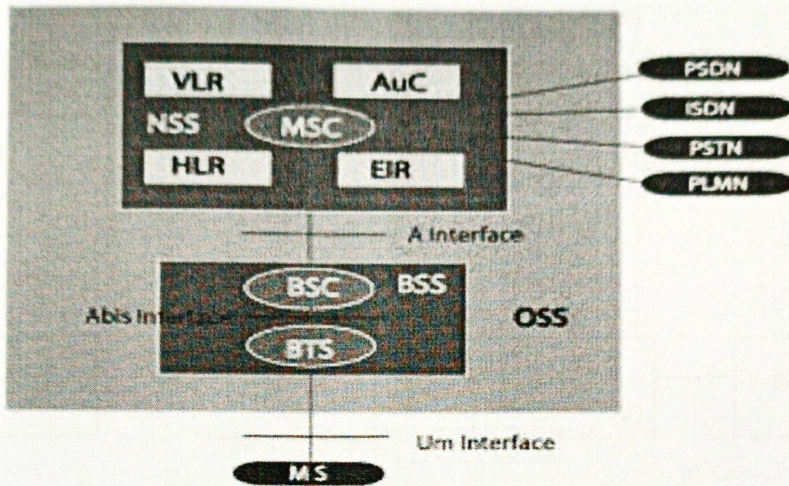
GSM is a cellular network, which means that cell phones connect to it by searching for cells in the immediate vicinity. There are five different cell sizes in a GSM network—macro, micro, pico, femto, and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base station antenna is installed on a mast or a building above average rooftop level. Micro cells are cells whose antenna height is under average rooftop level; they are typically used in urban areas. Picocells are small cells whose coverage diameter is a few dozen meters; they are mainly used indoors. Indoor coverage is also supported by GSM and may be achieved by using an indoor picocell base station, or an indoor repeater with distributed indoor antennas fed through power splitters, to deliver the radio signals from an antenna outdoors to the separate indoor distributed antenna system. These are typically deployed when significant call capacity is needed indoors, like in shopping centers or airports.

However, this is not a prerequisite, since indoor coverage is also provided by in-building penetration of the radio signals from any nearby cell.

GSM system was developed as a digital system using time division multiple access (TDMA) technique for communication purpose. A GSM digitizes and reduces the data, then sends it down through a channel with two different streams of client data, each in its own particular time slot. The digital system has an ability to carry 64 kbps to 120 Mbps of data rates.

4.1.6.1. GSM Architecture:

- **A Mobile Station:** It is the mobile phone which consists of the transceiver, the display and the processor and is controlled by a SIM card operating over the network.
- **Base Station Subsystem:** It acts as an interface between the mobile station and the network subsystem. It consists of the Base Transceiver Station which contains the radio transceivers and handles the protocols for communication with mobiles. It also consists of the Base Station Controller which controls the Base Transceiver station and acts as a interface between the mobile station and mobile switching centers .
- **Network Subsystem:** It provides the basic network connection to the mobile stations. The basic part of the Network Subsystem is the Mobile Service Switching Centre which provides access to different networks like ISDN, PSTN etc. It also consists of the Home Location Register and the Visitor Location Register which provides the call routing and roaming capabilities of GSM. It also contains the Equipment Identity Register which maintains an account of all the mobile equipment wherein each mobile is identified by its own IMEI number. IMEI stands for International Mobile Equipment Identity.



GSM - Architecture

- The network subsystem performs the switching of calls between
- The mobile users and other mobile and fixed network users

4.1.6.2.Future Of GSM:

GSM, together with other technologies, is part of an evolution of wireless mobile telecommunication that includes High-Speed Circuit-Switched Data (HSCSD), General Packet Radio System (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS).

4.1.7. POWER SUPPLY UNIT:

A power supply (sometimes known as a power supply unit or PSU) is a device or system that supplies electrical or other types of energy to an output load or group of loads. The term is most commonly applied to electrical energy supplies, less often to mechanical ones, and rarely to others.

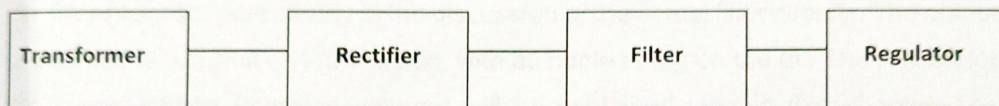


Figure 4.1.8 Block Diagram of Power Supply

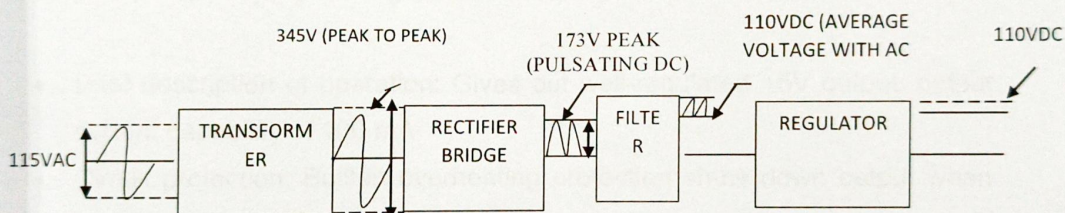


Figure 4.1.9 Processing of Power Supply

The transformer steps up or steps down the input line voltage and isolates the power supply from the power line. The RECTIFIER section converts the alternating current input signal to a pulsating direct current. However, as you proceed in this chapter you will learn that pulsating dc is not desirable. For this reason, a FILTER section is used to convert pulsating dc to a purer, more desirable form of dc voltage.

The final section, the REGULATOR, does just what the name implies. It maintains the output of the power supply at a constant level in spite of large changes in load current or input line voltages. Now that you know what each section does, let's trace an ac signal through the power supply. At this point you need to see how this signal is altered within each section of the power supply. Later on in the chapter you will see how these changes take place. An input signal of 115 volts ac is applied to the primary of the transformer.

The transformer is a step-up transformer with a turn's ratio of 1:3. You can calculate the output for this transformer by multiplying the input voltage by the ratio of turns in the primary to the ratio of turns in the secondary; therefore, $115 \text{ volts ac} \times 3 = 345 \text{ volts ac}$ (peak-to-peak) at the output. Because each diode in the rectifier section conducts for 180 degrees of the 360-degree input, the output of the rectifier will be one-half, or approximately 173 volts of pulsating dc. The filter section, a network of resistors, capacitors, or inductors, controls the rise and fall time of the varying signal; consequently, the signal remains at a more constant dc level. You will see the filter process more clearly in the discussion of the actual filter circuits. The output of the filter is a signal of 110 volts dc, with ac ripple riding on the dc. The reason for the lower voltage (average voltage) will be explained later in this chapter. The regulator maintains its output at a constant 110-volt dc level, which is used by the electronic equipment (more commonly called the load).

Simple 5V power supply for digital circuits

- Brief description of operation: Gives out well-regulated +5V output, output current capability of 100 mA
- Circuit protection: Built-in overheating protection shuts down output when regulator IC gets too hot
- Circuit complexity: Very simple and easy to build
- Circuit performance: Very stable +5V output voltage, reliable operation
- Availability of components: Easy to get, uses only very common basic components
- Design testing: Based on datasheet example circuit, I have used this circuit successfully as part of many electronics projects
- Applications: Part of electronics devices, small laboratory power supply
- Power supply voltage: Unregulated DC 8-18V power supply
- Power supply current: Needed output current + 5 mA
- Component costs: Few dollars for the electronics components + the input transformer cost

4.1.8. ARDUINO IDE

Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software , or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board.

The Arduino platform has become quite popular with people just starting out with electronics, and for good reason. Unlike most previous programmable circuit boards, the Arduino does not need a separate piece of hardware (called a programmer) in order to load new code onto the board – you can simply use a USB cable. Additionally, the Arduino IDE uses a simplified version of C++, making it easier to learn to program. Finally, Arduino provides a standard form factor that breaks out the functions of the micro-controller into a more accessible package.

The Arduino hardware and software was designed for artists, designers, hobbyists, hackers, newbies, and anyone interested in creating interactive objects or environments. Arduino can interact with buttons, LEDs, motors, speakers, GPS units, cameras, the internet, and even your smart-phone or your TV! This flexibility combined with the fact that the Arduino software is free, the hardware boards are pretty cheap, and both the software and hardware are easy to learn has led to a large community of users who have contributed code and released instructions for a **huge** variety of Arduino-based projects

There are many varieties of Arduino boards that can be used for different purposes. Some boards look a bit different from the one below, but most Arduinos have the majority of these components in common:

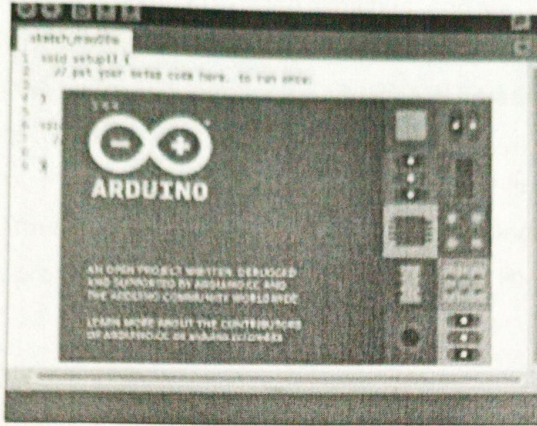
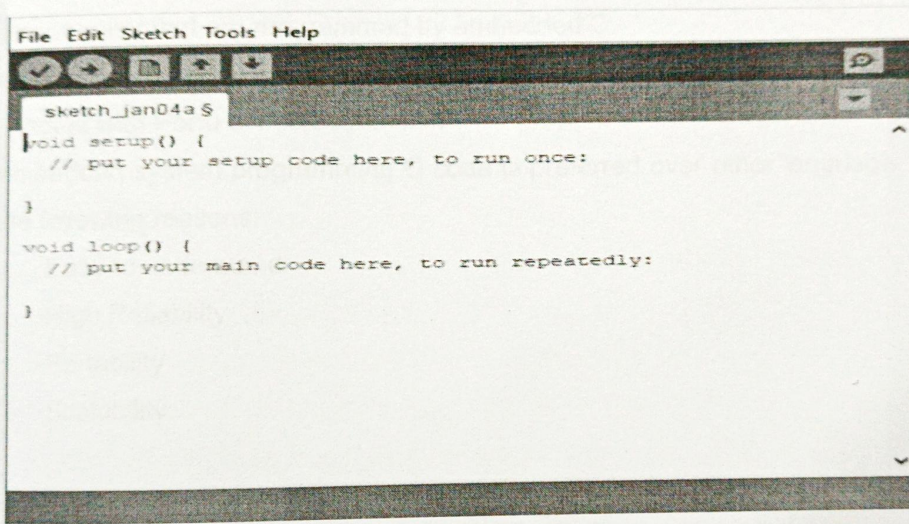


Figure 4.1.10 Arduino IDE Platform

Programs written using Arduino Software (IDE) are called **sketches**. These sketches are written in the text editor and are saved with the file extension `.ino`. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom righthand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor

The Arduino IDE is incredibly minimalistic, yet it provides a near-complete environment for most Arduino-based projects. The top menu bar has the standard options, including “File” (new, load save, etc.), “Edit” (font, copy, paste, etc.), “Sketch” (for compiling and programming), “Tools” (useful options for testing projects), and “Help”. The middle section of the IDE is a simple text editor that where you can enter the program code. The bottom section of the IDE is dedicated to an output window that is used to see the status of the compilation, how much memory has been used, any errors that were found in the program, and various other useful messages.

Projects made using the Arduino are called sketches, and such sketches are usually written in a cut-down version of C++ (a number of C++ features are not included). Because programming a microcontroller is somewhat different from programming a computer, there are a number of device-specific libraries (e.g., changing pin modes, output data on pins, reading analog values, and timers). This sometimes confuses users who think Arduino is programmed in an "Arduino language." However, the Arduino is, in fact, programmed in C++. It just uses unique libraries for the device.



The Arduino IDE supports the languages C and C++ using special rules of code structuring. The Arduino IDE supplies a software library from the wiring project, which provides many common input and output procedures. User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub *main()* into an executable cyclic executive program with the GNU Toolchain, also included with the IDE distribution. The Arduino IDE employs the program *avrdude* to convert the executable code into a text file in hexadecimal encoding that is loaded into the Arduino board by a loader program in the board's firmware.

4.1.9. EMBEDDED C:

Embedded C is most popular programming language in software field for developing electronic gadgets. Each processor used in electronic system is associated with embedded software.

Embedded C programming plays a key role in performing specific function by the processor. In day-to-day life we used many electronic devices such as mobile phone, washing machine, digital camera, etc. These all device working is based on microcontroller that are programmed by embedded C.

The Embedded C code written in above block diagram is used for blinking the LED connected with Port0 of microcontroller.

In embedded system programming C code is preferred over other language. Due to the following reasons:

- Easy to understand
- High Reliability
- Portability
- Scalability

Function is a collection of statements that is used for performing a specific task and a collection of one or more functions is called a programming language.

Most consumers are familiar with Application software that provide functionality on a computer. Embedded software however is often less visible, but no less complicated. Unlike application software, embedded software has fixed hardware requirements and capabilities, and addition of third-party hardware or software is strictly controlled.

Embedded software needs to include all needed device drivers at manufacturing time, and the device drivers are written for the specific hardware. The software is highly dependent on the CPU and specific chips chosen. Most embedded software engineers have at least a passing knowledge of reading schematics ,and reading data sheets for components to determine usage of registers and communication system. Conversion between decimal , hexadecimal and binary is useful as well as using bit manipulation.

Web applications are rarely used, although XML files and other output may be passed to a computer for display. File systems with folders are typically absent as are SQL databases.

Software development requires use of a cross compiler, which runs on a computer but produces executable code for the target device. Debugging requires use of an in-circuit emulator, JTAG or SWD. Software developers often have access to the complete kernel (OS) source code.

Size of the storage memory and RAM can vary significantly. Some systems run in 16 KB of Flash and 4 KB of RAM with a CPU operating at 8 MHz, other systems can rival contemporary computers. These space requirements lead to more work being done in C or embedded C++, instead of C++. Interpreted languages like BASIC (while e.g. Parallax Propeller can use compiled BASIC) and Java (Java ME Embedded 8.3 is available for e.g. ARM Cortex-M4, Cortex-M7 microcontrollers and older ARM11 used in Raspberry Pi and Intel Galileo

Gen. 2) are not commonly used; while an implementation of the interpreted Python 3 language – Micropython – is however available expressly for microcontroller use, e.g. 32-bit ARM-based (such as BBC micro : bit) and 16-bit PIC microcontrollers.

Communications between processors and between one processor and other components are essential. Besides direct memory addressing, common protocols include I²C, SPI, serial ports, and USB.

Communications protocols designed for use in embedded systems are available as closed source from companies including InterNiche Technologies and CMX Systems. Open-source protocols stem from uIP, lwip, and others

- This program explains how to use structure within structure in C using normal variable. "student_college_detail" structure is declared inside "student detail" structure in this program. Both structure variables Please note that members of "student_college_detail" structure are accessed by 2 dot(.) operator and members of "student are normal structure variables.
- _detail" structure are accessed by single dot(.) operator.

A Keyword is a special word with a special meaning to the compiler (a C Compiler for example, is a software that is used to convert program written in C to Machine Code). For example, if we take the Keil's Cx51 Compiler (a popular C Compiler for 8051 based Microcontrollers) the following are some of the keywords:

- bit
- sbit
- sfr
- small
- large

These are few of the many keywords associated with the Cx51 C Compiler along with the standard C Keywords.

4.2.ARCHITECTURE /OVERALL DESIGN OF PROPOSED SYSTEM:

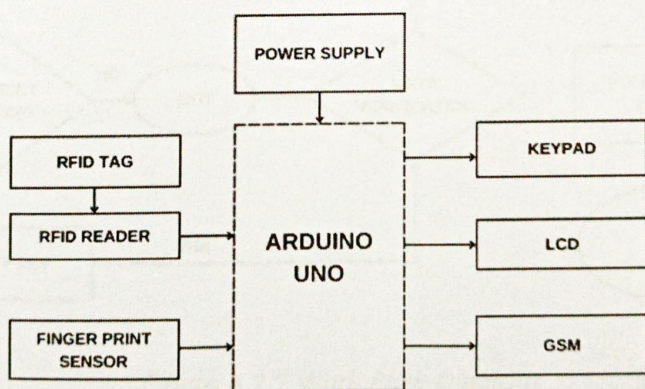


Figure 4.2.1 Architecture Diagram

It makes use of both radio frequency identification (RFID) and biometric authentication. Every voter's biometric information is recorded and saved during the admittance procedure together with other relevant papers. Every voter receives an RFID-based identity card when the admissions procedure is over. This ID card serves as the primary proof of identity for the election. The only people who are eligible to vote are those who have a valid ID card. During the voting process, the student spots the RFID card on the card reader. The second stage of authentication

is used to make sure the card belonged to the voter who is holding it. On the second level, the voting machine's fingerprint scanner verifies the student's biometric. The fingerprint in question is checked with the one that is recorded in the database. Only voters are allowed to cast votes if the entered password is accurate. After the voting process is finished an message will be sent successfully

4.3.WORK FLOW METHOD:

WORK FLOW DIAGRAM

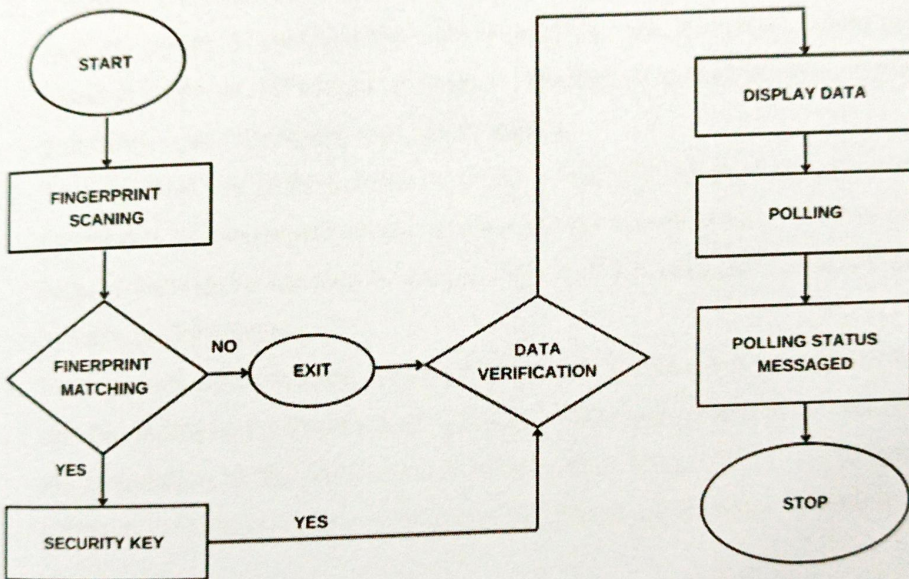


Figure 4.2.2 Work Flow Diagram

- Step 1: The voter should place their fingerprint on the fingerprint sensor.
- Step 2: If the fingerprints match, enter the provided security key.
- Step 3: After the two authentication processes have been completed, the LCD displays the user's information.
- Step 4: The voter can place their respective votes.
- Step 5: The polling status message will be sent to their registered mobile number.

CHAPTER 5

IMPLEMENTATION DETAILS

5.1.DEVELOPMENT AND DEPLOYMENT SETUP:

1. **Hardware Setup:** Gather all the necessary hardware components such as an Arduino board, a TFT touchscreen display, an RFID reader, a fingerprint scanner, and any other required components. Assemble the hardware according to the system design specifications.
2. **Software Development:** Develop the software program that will run on the Arduino board to perform the voting process. The program should include features such as RFID authentication, fingerprint authentication, candidate selection, vote recording, and result tallying.
3. **Testing:** Test the AVM system to ensure that it is functioning properly and meets the requirements of the system design specifications. Testing should include testing the hardware components, software program, and the overall system performance.
4. **Deployment Setup:** Once the AVM system has been tested and verified, it can be deployed for the student elections. The deployment setup will include the installation of the AVM system in the voting area, setting up the network connection if required, and configuring the database for voter information and vote tallying.
5. **Training and Support:** Provide training to the election officials and students on how to use the AVM system. Offer technical support throughout the election process to ensure that the system is functioning properly and to address any issues that may arise.
6. **Post-Election Procedures:** After the election, the votes will be tallied and the results announced. Ensure that the results are accurate and that the AVM system is properly shut down and stored for future use.

5.2.TESTING :

1. Unit Testing: Test each component of the AVM system, including the RFID reader, fingerprint scanner, and the software program to ensure they are functioning properly. Conduct unit testing for each component individually before moving on to integrated testing.
2. Integration Testing: Test the AVM system as a whole to ensure that all components work together properly. Conduct integration testing by simulating the voting process and testing each component's interaction with the others.
3. Performance Testing: Test the system's performance to ensure that it can handle the expected load during the election process. Performance testing should include testing for response time, transaction throughput, and system availability.
4. Security Testing: Test the system's security features to ensure that it is secure from hacking attempts and unauthorized access. Conduct security testing by attempting to break into the system and testing the system's ability to detect and prevent unauthorized access.
5. Usability Testing: Test the system's usability by simulating the voting process and testing how easily voters can navigate the system. Conduct usability testing with a group of users and gather feedback to improve the system's user experience.
6. End-to-End Testing: Conduct end-to-end testing to ensure that the system functions correctly from start to finish. This testing includes testing the entire voting process from voter authentication to vote tallying.
7. Acceptance Testing: Once all testing is complete, conduct acceptance testing to ensure that the AVM system meets the system design specifications and requirements. This testing should include a final review of the system's performance, usability, security, and accuracy.

CHAPTER 6

RESULT AND DISCUSSION

1. **Increased Security:** The AVM system using RFID and fingerprint technology offers higher security features than traditional paper-based voting systems. This is because the system can only be accessed by authorized voters using their RFID cards and biometric data, preventing unauthorized access and vote manipulation.
2. **Efficient and Accurate:** The AVM system is efficient and accurate in recording and tallying votes, reducing the time taken to declare election results. The system automatically records the votes in real-time, eliminating the need for manual counting, which can result in errors and time-consuming.
3. **User-Friendly:** The AVM system is user-friendly and easy to navigate for voters. The touchscreen display and intuitive interface make it easy for voters to select their candidates and cast their votes.
4. **Transparency:** The AVM system promotes transparency in the voting process by ensuring that every vote is recorded and tallied accurately. This can increase voter confidence in the election process.

CHAPTER 7

CONCLUSION

In this paper, the authors presented an intelligent and secure authenticated voting system based on The Arduino flat-form IoT technology for college elections To ensure voter safety and security To preserve the sanctity of the method, a two-layer security scheme is introduced. We assume this method is useful in conducting fair and open student council elections for schools. Although the system .Although it produces the expected performance and efficiency, it is not 100% perfect. Some limitations of the system has been found. The system is supporting only three candidates at a time as it has only three voting switches. This can be addressed in our future work. Further, the system enables the election to. At any given time, there is only one post .We can design the system such that it can be used to conduct elections to any number of posts at the time. One more point is that the Arduino Mega board has limited memory. In our future work, we are planning to use a Raspberry Pi-based board of the AVM. The devices built into this. To speed up the process, the project can be updated, and the data can be stored in the cloud server with automated voting. start the voting process. As the system is in its infancy, more work is necessary to make it versatile and more adaptable. It is in beta; we will present a device that is upgraded, error-free, stable, and scalable.in our future work.

REFERENCES:

- [1] Arooj and M. Riaz, "Electronic voting with biometric verification offline and hybrid EVMs solution," 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland, 2016, pp. 332-337, doi: 10.1109/INTECH.2016.7845009.
- [2] V. K. Priya, V. Vimaladevi, B. Pandimeenal and T. Dhivya, "Arduino based smart electronic voting machine," 2017 International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, India, 2017, pp. 641-644, doi: 10.1109/ICOEI.2017.8300781.
- [3] H. Agarwal and G. N. Pandey, "Online voting system for India based on AADHAAR ID," 2013 Eleventh International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, 2013, pp. 1-4, doi: 10.1109/ICTKE.2013.6756265.
- [4] J. Deepika, S. Kalaiselvi, S. Mahalakshmi and S. A. Shifani, "Smart electronic voting system based on biometrie identification-survey," 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM), Chennai, India, 2017, pp. 939-942, doi: 10.1109/ICONSTEM.2017.8261341.
- [5] Mansingh, P. M. B., Titus, T. J., & Devi, V. S. S, 2020, A Secured Biometric Voting System Using RFID Linked with the Aadhar Database. 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020. 1116–1119
- [6] S. Lavanya, "Trusted secure electronic voting machine," International Conference on Nanoscience, Engineering and Technology (ICONSET 2011), Chennai, India, 2011, pp. 505-507, doi: 10.1109/ICONSET.2011.6168014.
- [7] R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo and M. A. Rahman, "Biometrically secured electronic voting machine," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 2017, pp. 510-512, doi: 10.1109/R10-HTC.2017.8289010.
- [8] K. Weldemariam, R. A. Kemmerer and A. Villafiorita, "Formal Specification and Analysis of an E-voting System," 2010 International Conference on Availability,

Reliability and Security, Krakow, Poland, 2010, pp. 164-171, doi: 10.1109/ARES.2010.83.

[9] D. A. Kumar and T. U. S. Begum, "Electronic voting machine — A review," International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012), 2012, pp. 41-48,

[10] Firas Hazzaa¹, Seifedine Kadry, "New System of E-Voting Using Fingerprint (2012)", International Journal of Emerging Technology and Advanced Engineering (IJETA) Volume 2, Issue 10, pg. 355- 363.

[11] Ashok Nalluri, B. BhanuTeja, A. Balakrishna, "RFID and Fingerprint Recognition based Electronic Voting System for Real Time Application (2014)", International Journal of Engineering Development and Research (IJEDR), Volume 2, Issue 4, pg. 3850- 3854,.

[12] B. Zhang and H.-S. Zhou, "Statement voting," Financial Cryptography and Data Security 2019, 2019.

[13] SpurthiAnjan, Johnson P Sequeira "Blockchain Based E-Voting System for India Using UIDAI's Aadhaar" Journal of Computer Science Engineering and Software Testing, e-ISSN: 2581-6969 Volume 5 Issue 3, 2019.

[14] Rifa Hanifatunnisa, et al, "Blockchain Based EVoting Recording System Design", School of Electrical Engineering and Informatics 2017

[15] Election Commission of India , Status Paper on Electronic Voting Machine [IEEE] , April 2017.

[16] Galaburdina A. (March 29, 2018). "USA Introduces Blockchain For Election Voting". Available at: <https://jourtify.com/ssha-vnedrjaet-blokchejn-dlja-golosovanija-na-vyborah/> (Accessed April 09, 2019). (in Russian

[17] K. Kim ,J. Kim, B. Lee, and G. Ahn , "Experimental design of worldwide internet voting system using pki," 2001.

[18] Navya A et al. "Electronic voting machine based on Blockchain technology and Aadhar verification "International Journal of Advance Research, Ideas and Innovations in Technology, ISSN: 2454 -132X (Volume 4, Issue 2), 2018.

[19] Diponkar Paul and Sobuj Kumar Ray, A Preview on Microcontroller Based Electronic Voting Machine International Journal of Information and Electronics Engineering, Vol. 3, No. 2, March 2013.

[20] Vanessa Teague, Steve Schneider, Peter Y.A. Ryan, "End to End Verifiability in voting system from theory to practice" June- 2015

[21] R.Murali Prasad, et al, "AADHAR based Electronic Voting Machine using Arduino", International Journal of Computer Applications, vol.145, no. 12, July 2016.

APPENDIX

SCREENSHOTS

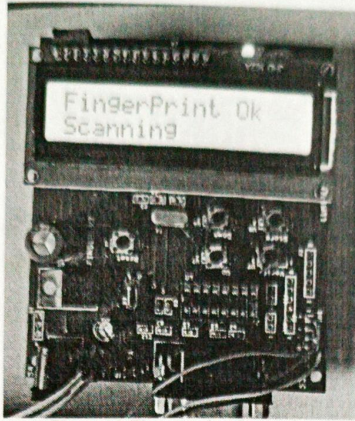


Figure 1.Fingerprint Scanning

The person places their fingerprint on a scanner, which captures an image of the fingerprint. The scanner then converts the image into digital format, which can be analysed by a computer. The computer checks the fingerprint with the databases collected to identify the person.

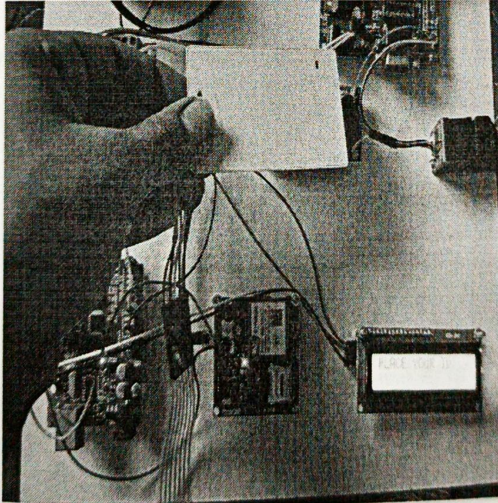


Figure 2.RFID Scanning

The RFID scanner emits a radio signal that activates the electronic chip in the RFID card. The chip in the card responds to the scanner's signal by transmitting its unique identification information back to the scanner. The computer system then uses the information to identify the user and perform the necessary action.

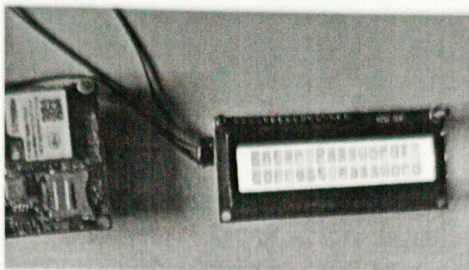


Figure 3.Password Authentication

Then the person is asked to verify with password authentication, where the user is given a 4-digit password with their RFID card.

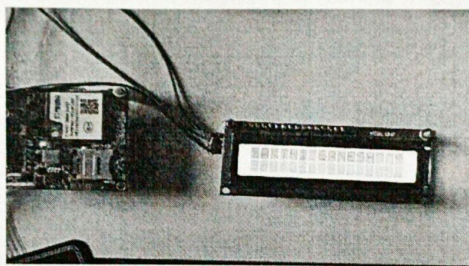


Figure 4.Identify the user

After the authentication process has been completed, the LCD displays the user name.



Figure 5.Voting Process

The LCD displays the voting options, and the voter can cast their vote for the respective candidates.

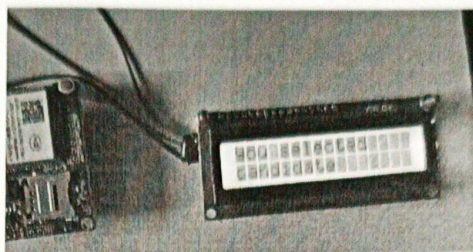


Figure 6.Candidate Selected

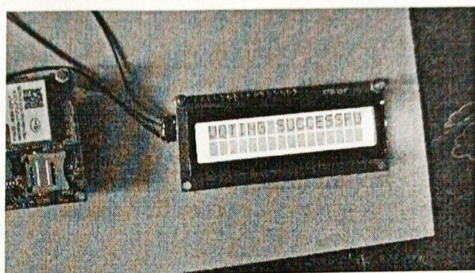


Figure 7.Voting Completed

After the voting process has been completed, the LCD displays a "voting successful" message.

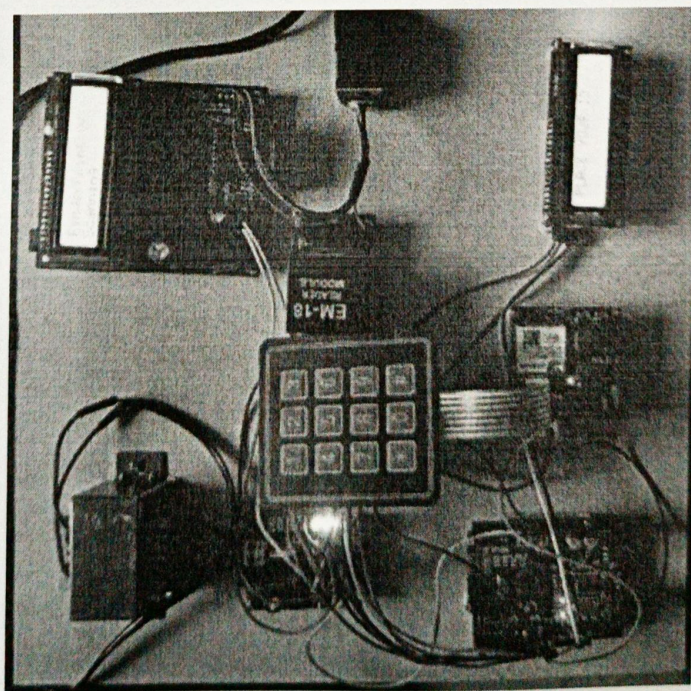


Figure 8.Whole Voting Setup