AADHAAR BASED ELECTRONIC VOTING SYSTEM AND AUTHENTICATION ON INTERNET OF THINGS

[1]THIYAGESAN M, [2]JAYA LEKSHIMI M, [3]KANMANI P, [4]PRIYANKA A

[1]Assistant Professor, [2, 3, 4] UG-Scholar, Department of Electrical and Electronics Engineering,

R.M.K. Engineering College, Thiruvallur, Chennai.

Email: [1] thiyagesanm@gmail.com, [2] jayjanu97@gmail.com

Abstract--**"Electronic Voting Machine" has become an effective tool nowadays. People are assured that their vote is secured and this is the reason it becomes more widespread. This paper is proposed to provide a secure Electronic Voting system using Fingerprint Identification method by accessing the AADHAAR card database by scanning the QR code. The voted data and voters details can be sent to the nearby Database Administration unit through WIFI system. The fingerprint scanning is used to avoid fake and repeated voting. The databases are effectively verified and monitored by PIC microcontroller. The purpose of this system is to ensure that the voting rights are accessed only by the legitimate user and avoids bogus voting, which will provide secure democracy of voting and also improves the percentage of efficient voting.**

Keywords*: *Fingerprint Identification, AADHAAR card, QR code, WIFI, PIC microcontroller

I. INTRODUCTION

After getting freedom from the British government, Indian Government provides a right to Indian people to elect their interested leader. For conducting and controlling voting in India, a separate commission was introduced, which was named as Election Commission of India (ECI). This commission is not favorable or support to any political party. As per rules of law, this commission works. For the persons, whose age is18 and above are eligible to enroll their vote. Around the world, voting systems include identification of voter, recording of the casted vote, counting of the vote, an announcement of election results. Voter identification is required during two phases of the electoral process: first for voter registration in order to establish the right to vote and afterward, at voting time, allowing the citizen to cast their vote by verifying (authentication). Security is a heart of e-voting process. Hence it is necessary for designing a secure electronic voting system is very important.

Thus, it ensures the security and privacy but it is time-consuming, expensive, and inconvenient for voters. There are different levels of e-voting security. Therefore serious measures must be taken to keep it out of public domain. Also, security must be applied to hide votes from publicity. Firstly the voters AADHAAR Card QR code is scanned in the QR scanner. The scanned code database is transferred to the Microcontroller unit through Bluetooth module, hence, it will send the data obtained from the card to the Microcontroller. The Microcontroller (is connected to the central server where all information of AADHAAR Cardholders has been stored already) access the data stored in its memory by the code obtained from the code. Now, the voter can be subjected to fingerprint test to validate the details of the voter in case of any discrepancy found in the photo due to aging etc. When system reads the voter's id from the fingerprint, the system creates a fake id and updates in the database. This is helpful in counting the total vote comparing to total citizens voted. This way we can rule out the fraud voting. If the voter is not eligible or not validate to vote a buzzer indication will be given and The LCD display is provided in the system to guide and instruct the voter to make the voting procedure more convenient.

II. EXISTING SYSTEM

Electronic Voting Machine (EVM) was invented by M.B. Hafeena which was used on the experimental basis in India during 1989-1990 in 16 Assembly Constituencies. Today, about two dozen nations have adopted electronic voting. [1] Thus, on this landscape, India is undoubtedly a world leader. [1] India stands out as the largest democracy in the world which has hundred percent electronic voting. [1] There are many countries which adopted electronic voting and but now they were forced to go back to a paper balloting system. [1] This

unique standalone nature of the machines which give them the necessary make them as tamper-proof as any machine can really be.[1] In a judgment, the Karnataka High Court called the EVM as a "national pride" and also acknowledged the Indian election system as a "global gold standard".[1]

A. Working of EVM

Existing EVM is capable of enrolling 3840 whereas each polling station has the maximum of 1500 votes and it can hold up to 64 candidates. It works with the supply of 6 Volt alkaline batteries.

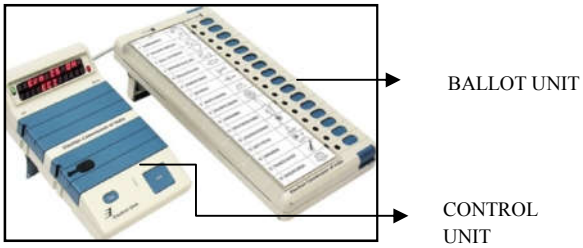

FIG 1 ELECTRONIC VOTING MACHINE

This system consists of two units-Controls Unit, Balloting Unit. The units are interfaced through five-meter cable. The balloting unit is placed for voters' interface, in which the voters will cast their vote and the control unit, will be under the Polling Officer monitoring. The vote is cast by pressing the blue button on the Balloting Unit for the respective candidate and symbol of his choice. Instead of using a ballot paper, the Polling Officer, who is in-charge of the Control Unit will be pressing the Ballot Button. This will enable the voter to cast his vote. The control unit is the main unit which stores all data and controls the functioning of EVM.

B. Problems in Existing System

- Improper validation of voters, as it is done manually.
- Capturing of Polling Booth.
- Even brief access to the machine could allow altering the election results.
- Constant spending funds for the elections staff are provided.
- The EVMs can be easily manipulated by using additional hardware to the control unit circuit board that could read and write the EEPROM chips thereby record the vote that has been cast by the people.
- Also, there exist no procedures for voters to verify their vote and ensure transparency. So, the proposed electronic voting system has to be addressed with these problems.

III. PROPOSED SYSTEM

A. Block Diagram Representation

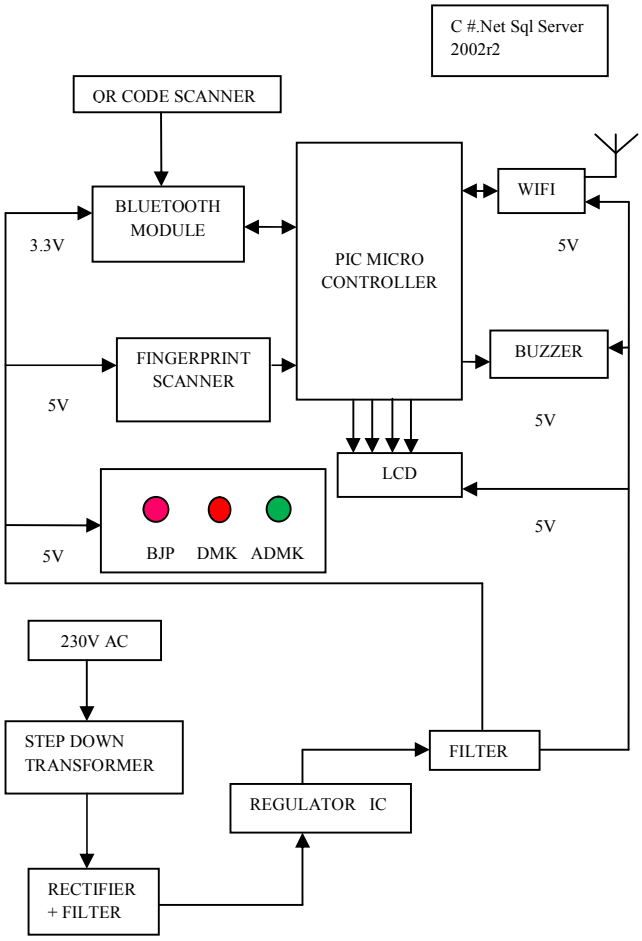

FIG 2 BLOCK DIAGRAM OF PROPOSED SYSTEM

The QR code in the AADHAAR Card is scanned through the QR scanner by mobile application. The scanned data is transmitted the PIC microcontroller through the Bluetooth Module EGBT-045MS. The data is now transmitted through WIFI from PIC microcontroller to the Central Server Station and the data is accessed and verification is done. The LCD displays "PLACE THE FINGER IN SCANNER". Now, the fingerprint is scanned by the Fingerprint Scanner R305 and the scanned data is transmitted to the PIC microcontroller and the d fingerprint data is verified by comparing with the Fingerprint template stored in the AADHAAR database which is accessed through WIFI. Now, the LCD displays "VERIFIED" "PLEASE VOTE" and after casting the vote, it displays "THANK YOU".

After verification, the voter is allowed to cast his/her vote. The vote will be counted and stored in the Memory of PIC microcontroller which can be retrieved after the election. If the voter is not eligible or not valid to cast the vote buzzer will alarm during verification either while QR code database verification or during fingerprint verification and LCD displays "INVALID". If the voter is already cast his vote then LCD displays "ALREADY VOTED". The supply for overall system is provided by rectifying and regulating unit. The 230v AC supply is stepped down by the transformer and rectified to DC supply by rectifier and harmonics are removed through the filter and regulated by the regulator for the desired voltage of 5V. The supply of 5V regulated DC supply is given to the entire system.

B. Hardware Components

The Hardware Components of the proposed system are

1. Bluetooth Module
2. Fingerprint Scanner
3. PIC Microcontroller
4. LCD Display
5. WIFI Module
6. Buzzer
7. Regulated Power Supply Unit

1. BLUETOOTH MODULE

EGBT-045MS and EGBT-046S are Bluetooth Modules which are loaded with Service Pack for ProLiant (SPP) firmware for UART wireless cable replacement functions to make the system simple. This module can be configured to work either as a master or slave Bluetooth device by using a set of commands. EGBT-046S, on the other hand, is permanently programmed as Bluetooth slave device. EGBT-046S has the simpler function, is a lot easier to use, and of course, costs less than EGBT-045MS. The EGBT-04 module will work with the supply voltage of 3.1VDC to 4.2VDC.

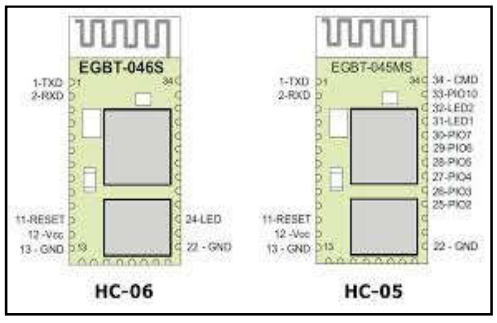

FIG 3 BLUETOOTH MODULE PIN DIAGRAM

When supplied with 3.3VDC, it will interface directly with the UART port of any microcontroller chip running at 3.3VDC. When used with 5V microcontrollers, The TXD output logic swing of the EGBT-04 still falls within the valid 5V TTL range, hence, can be connected directly to the UART RXD of the 5V microcontroller host. [2] This module is employed to transfer the scanned data of QR code to the PIC microcontroller.

2. FINGERPRINT SCANNER

R305 biometric fingerprint reader/sensor module build with TTL UART interface can be used for direct connections to a microcontroller UART. This module can directly interface with any 3.3V or 5V microcontrollers. Fingerprint processing includes enrollment of fingerprint data and fingerprint verification. While enrolling, the user needs to register his/her finger two times to generate a template of the finger based on the processing. For verification, the user scans his/her finger again through the optical sensor and the system will generate a duplicate image of the finger and compare it with templates in the library. The verification can be 1:1 matching, in which the system will compare the live finger with template designated in the Module. The verification can be also 1: N matching, or searching, where the system will search the whole finger library for the matching finger. The system will return the verified result. [3] In our proposed system Enrollment or creation of Template is not needed to be done as the fingerprint is compared with AADHAAR database stored in PIC microcontroller which is accessed through WIFI.

FIG 4 R305 FINGERPRINT MODULE

a. Features

- Integrated image collecting, algorithm chip together.
- Low power consumption—Voltage:3.6-6.0 V DC, Working current: Typical 90 mA, Peak 150mA
- low cost, small size, excellent performance
- Professional optical technology.
- Good image processing capabilities

3. PIC Microcontroller

Peripheral Interface Controller (PIC) microcontroller chips are the world's smallest microcontrollers. Microcontrollers are designed for embedded applications that make the embedded world very simple. It includes Processor for processing, Non-volatile memory for the program (ROM or flash), Volatile memory for input and output (RAM), Clock

for timer and counter and Control unit for controlling the system process. It is also called as “computer on a chip”.

a. Reasons for using PIC

- Variety of choices (8-bit to 32-bit)
- Affordable (Low Cost)
- Low Power
- Reasonable Size
- Convenient Packaging
- Through Hole (Dip)
- Surface Mount (SMD)

b. ANALOG TO DIGITAL CONVERTER MODULE

When configuring and using the ADC there are some functions to be considered: Port configuration, Channel selection, ADC voltage reference selection, ADC conversion clock source, Interrupt control, Results from formatting Port configuration. The ADC can be used to convert both analog and digital signals. The ADC plays a major role in fingerprint verification process.

4. LCD Display

LCD (Liquid Crystal Display) is an electronic display module which finds a wide range of applications in the digital environment for every display unit due to its uniqueness. A 16x2 LCD can display 16 characters in a line of 5x7 pixel matrix each and has totally 2 lines in it. The command register stores the command instructions. To do a predefined task like initializing the LCD for display, positioning the cursor, clearing the screen, controlling display features like brightness, contrast etc., and the instructions are given to the command registers. The data register stores the data that has to be displayed on the LCD. The LCD controller requires about 40 to 120 microseconds for writing and reading and needs 5 milliseconds for other operations. LCD requires 11 Input/output supply lines of 5 Volts for 8-bit data.

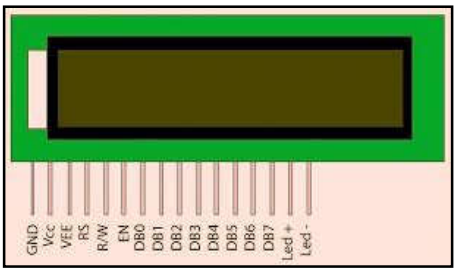

FIG 5 LCD PIN DIAGRAM

5. WIFI Module

ESP8266 is WIFI module suitable for connecting to an existing microcontroller project via a UART serial connection without altering the process and function of the microcontroller. The hardware connections required to connect are almost simple and straight-forward. This module needs only 3.3V power.

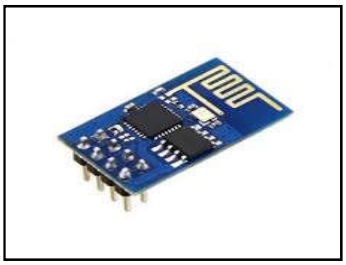

FIG 6 ESP8266 WIFI MODULE

a. Features

- It has Integrated temperature sensor
- Power down leakage current is less than 10uA
- Integrated low power 32-bit CPU could be used as application processor
- Serial Peripheral Interface, Universal Asynchronous Receiver Transmitter
- Standby power consumption of is less than 1.0mW

6. Buzzer

Nowadays Magnetic buzzers are available in both transducer and indicator configurations. The transistor acts as the driving circuit in a magnetic buzzer. The transistor creates a tone when a dc voltage is applied to it. On the other hand, a magnetic buzzer can be driven to generate 85 dB by only 1.5V, but the consumption of the current will be much higher than Piezo one. Narrow operating voltage: 1–16V. Higher current consumption: 30–100mA. Lower-rated frequency. Smaller footprint and Lower sound pressure level.

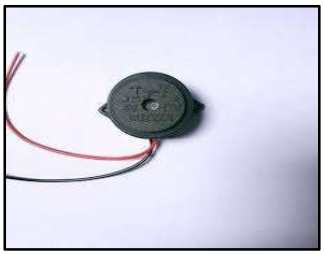

FIG 7 BUZZER

7. Regulated Power Supply

The Regulated power supply is an electronic circuit that is designed to converts unregulated AC into a constant DC.

With the help of a rectifier, it converts AC supply into DC. The regulated power supply has the main function, which is to supply a stable voltage, which has to be operated within certain limits. The output from the regulated power supply may be linear or pulsating but is nearly always DC.

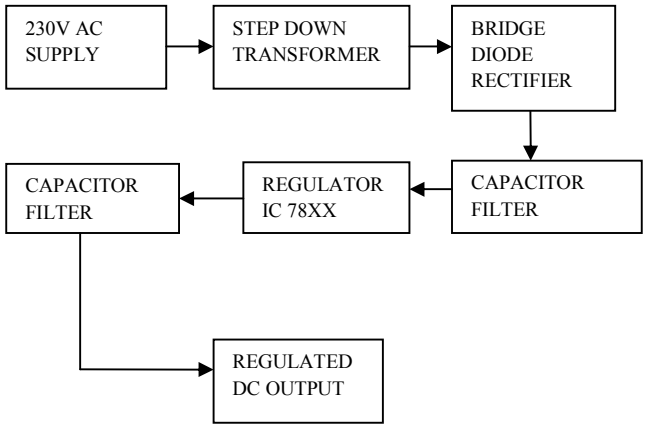

FIG 8 BLOCK DIAGRAM OF REGULATED SUPPLY

a. Step down Transformer

The Transformer transforms the electrical power from one circuit to another without a change in frequency. It is also known as "Static Device". A Step-down Transformer steps down the input voltage i.e. the secondary voltage is less than the primary voltage. The stepped down voltage is AC waveform.

FIG 9 STEP DOWN TRANSFORMER

b. Bridge Diode Rectifier

The Rectifier is the device which converts (bidirectional) alternating AC voltage to (pulsating) varying DC unidirectional voltage. As the term indicates it rectifies the portion of the alternating signal and provides a unidirectional signal at the output. This is done by the semiconductor diode. The semiconductor diode allows the signal in only one direction and blocks the signal in reverse direction. Bridge Diode Rectifier has four rectifier diodes which are arranged in the form of bridge in which two diodes conduct for one half AC cycle and the pulsating DC output with two pulses per cycle is provided.

FIG 10 BRIDGE DIODE RECTIFIERS

c. Capacitor Filter

The output of the rectifier is unidirectional DC current which has pulsating (variation in) magnitude. The Filter is the devices which convert the pulsating DC to pure DC. It filters the oscillations in the signal and provides a pure DC at the output. The capacitor stores the electrical energy for a short time and discharges it. Thereby controlling the charging and discharging rate of the capacitor the pure DC can be obtained. The capacitor is connected parallel to the power supply to filter out the AC component and thus DC will reach the load.

d. Regulator

Voltage regulator IC maintains the output voltage at a constant value. It is employed as voltage sources in a circuit which may have fluctuations. 78xx series is a fixed linear voltage regulator ICs which is used to maintain fluctuations voltage in a linear manner, 7805 IC, is a voltage regulator integrated circuit (IC) a member of this family. The xx in 78xx indicates the fixed output voltage it provides. 7805 IC provides +5 volts regulated power supply with provisions to add heat sink as well.

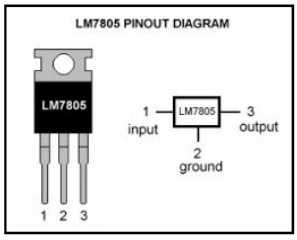

FIG 11 REGULATOR IC 7805

The regulated voltage is again filtered to eliminate the harmonics and the pure DC is given as supply to the system.

C. Software System

The software plays a major role in our proposed system. The security of the AADHAAR based voting relays on

software. The Code Composer Studio (CCS) is the coding software which is employed in our proposed system and PROTEUS 7.0 is used for the simulation purpose. The proposed system is an embedded based system for which programming software can be easily done by CCS. The CCS C language is used for programming. The simple form of our program is explained below through the flowchart.

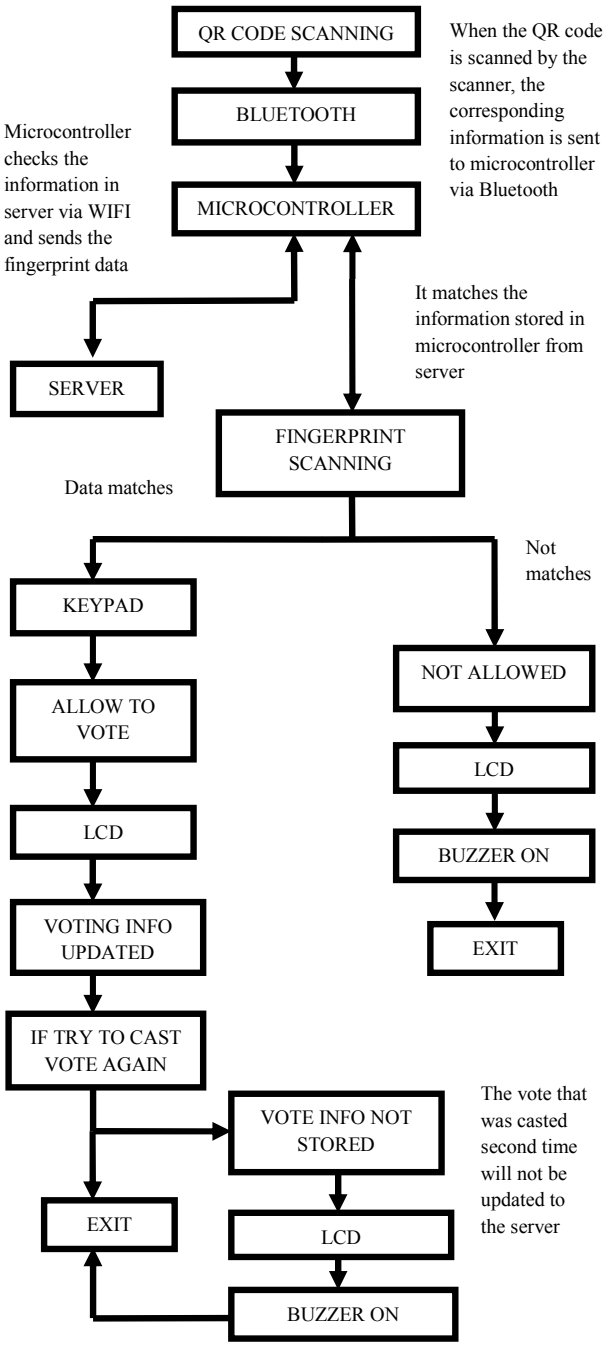

FIG 12 FLOWCHART OF THE SOFTWARE OF PROPOSED SYSTEM

D. Simulation Results

The case study for the proposed system is done by using the simulation. The software Proteus 7.0 is used for our simulation.

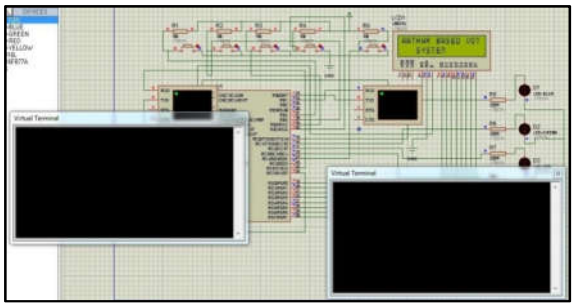

FIG 13 SIMULATION CIRCUIT OF PROPOSED SYSTEM

The above figure shows the circuit schematic representation of our proposed system. The virtual terminal at right side shows the representation of fingerprint scanner and the virtual terminal at left side shows the QR code scanner. The required program for microcontroller and for the other components is uploaded.

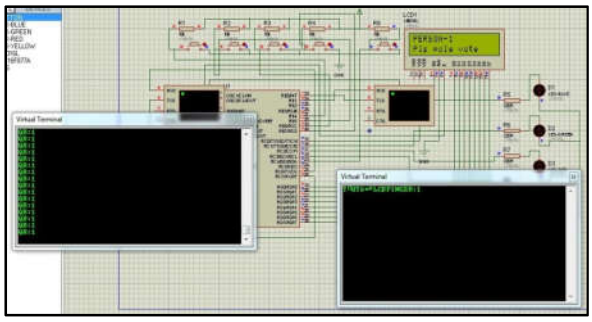

FIG 14 SIMULATION RESULT OF AUTHENTICATION

The above simulation result shows that when QR code scanner for person 1 is done it verifies it through fingerprint scanner from the database. Once when it is verified the LCD instructs the person to vote.

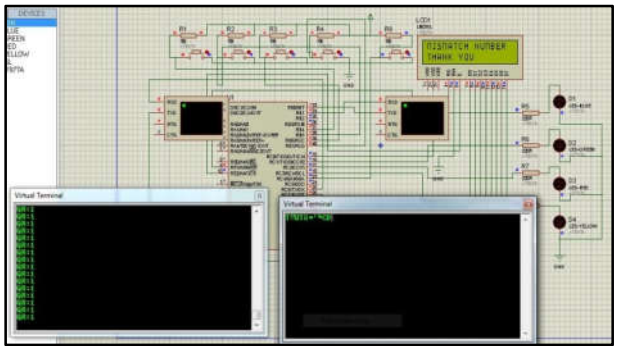

FIG 15 SIMULATION RESULT FOR MISMATCH AUTHENTICATION

When the authentication fails during fingerprint scanning the LCD displays as “MISMATCH” and buzzer alarms. Thus the authentication is secured and avoids illegal voting. After verification, the voters can cast their vote. If the voters try to do repeated voting LCD displays “voted” and the buzzer alarms. Thus repeated voting is avoided. In the simulation, the buzzer alarm cannot be shown hence an LED is given which glows.

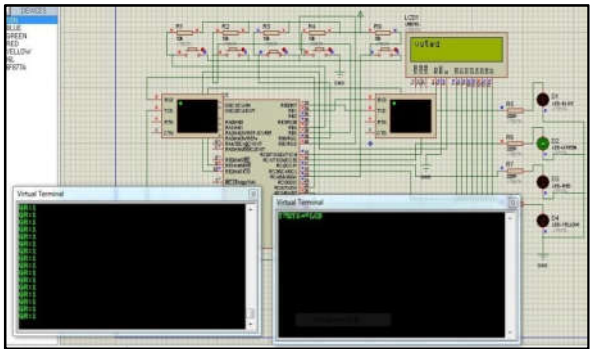

FIG 16 SIMULATION RESULT FOR REPEATED VOTING

III. CONCLUSION

In this paper, we have proposed a voting system which is better and faster due to the employment of biometrics. The present scenario of the voting system is studied in detail. The various components and the software that is involved in our proposed system are explained. The power supply is also chosen by studying in detail. The objectives of this system are to prevents illegal voters, provides ease of use, transparency for voters and maintains the integrity of the voting process which is all verified by various case studies that are done through simulation. The system also prevents multiple votes by the same person and checks the eligibility of the voter which is also shown through simulation. AADHAAR based Electronic voting systems have many advantages over the traditional way of voting as it involves the personal authentication through biometrics. Future enhancements focused to design a system which can be easy to use and will provide security and privacy of votes on the acceptable level by concentrating the authentication and processing section with more economical and secure manner.

IV. REFERENCE

[1]. http://www.livemint.com/Politics/QqVCQr55MrEzZvslEsUJzN/Why-India-stands-out-as-a-gold-standard-in-electronic-voting.html

[2]. e-Gizmo Mechatronix Central EGBT-046S/EGBT-045MS Bluetooth http://egizmo.net/oc/kits%20documents/HC05%20Bluetooth%20Module%20breakoutboard/EGBT-045MS-046S%20Bluetooth%20Module%20Guide.pdf

[3].http://www.electroschematics.com/11944/how-to-use-fingerprint-identification-modules/

[4]. D. Ashok Kumar, T. Ummal Sariba Begum A Novel design of Electronic Voting System Using Fingerprint International Journal of Innovative Technology & Creative Engineering (Issn: 2045-8711) Vol.1 No.1 January 2011

[5]. Kashif Hussain Memon, Dileep Kumar, and Syed Muhammad Usman, Next Generation A Secure E-Voting System Based On Biometric Fingerprint Method 2011 International Conference On Information And Intelligent Computing IPCSIT Vol.18 (2011)

[6]. Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, Richard A. Kemmerer, William Robertson, Fredrik Valeur, And Giovanni Vigna, An Experience In Testing The Security Of Real-World Electronic Voting Systems Ieee Transactions On Software Engineering, Vol. 36, No. 4, July/August 2010

[7]. Barbara Ondrisek E-Voting System Security Optimization Proceedings of The42nd Hawaii International Conference on System Sciences – 2009

[8]. Hari K. Prasad Arun Kankipati Sai Krishna Sakhamuri Vasavya Yagati Netindia, Security Analysis of India’s Electronic Voting Machines Scott Wolchok Eric Wustrow J. Alex Halderman The University of Michigan Hyderabad

[9]. HristinaMihajloska, Vesna Dimitrova and Ljupcho Antovski Security Aspects of Electronic Voting Systems Cyril and Methodius University Faculty of Natural Sciences and Informatics Institute of Informatics, Skopje, Macedonia

[10]. Xuejun Tan∗, Bir Bhanu Fingerprint matching by genetic algorithms Center for Research in Intelligent System, University of California, Riverside, CA 92521, USA Received 24 February 2004; accepted 6 September 2005

[11]. Bernd Heisele, a, b, Purdy Ho,c Jane Wu,b and TomasoPoggiobFace recognition: component-based versus global approaches Received 15 February 2002; accepted 11 February 2003

[12]. Implementation of Biometric Voting Machine Using Aadhaar Card Gowri, Guruprasanth, Jaya Surya. D, Krishnan. S, Dhanasekaran. S 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN: 2394-4099 Themed Section: Engineering and Technology