FQ Based Electronic Voting Machine Using Raspberry Pi With Aadhar

Prof Mr.S.Balakrishnan[1], Surya A[2], Gowthaman K[3], Tamizharasan K[4]

[1]Asst,Prof., Dept of Electronics and Communication Engineering
[2, 3, 4]Dept of Electronics and Communication Engineering
[1, 2, 3, 4] TheKavery Engineering College,Mecheri,Salem

Abstract- *This paper includes the updated version of EVM(Electronic Voting Machine) for real time purpose with high security. There are two authentication stages in this project. First authentication stage is QR(Quick Response) scanner . Second stage is fingerprint matching. During the election period, the QR code scanner is used to scan the Aadhar card for temporary stored. Next, the citizen's fingerprint is sensed using fingerprint module and it is searched in the data base which is predefined for matching purpose of the same citizen. Then the citizen's face is captured by the camera for the future purpose. Then the citizen can vote on the electronic ballot. If unauthorized citizen votes then the buzzer alerts.*

Keywords- EVM, Fingerprint, QR, Face capture.

I. INTRODUCTION

The electronic voting machines have been used in all general and state assembly elections of India since 2004.Prior to the introduction of electronic voting, India used paper ballots and manual counting.The paper ballots method was widely criticised because of fraudulent voting and booth capturing, where party loyalists captured booths and stuffed them with pre-filled fake ballots.The printed paper ballots were also more expensive,requiring substantial post-voting resources to count hundreds of millions of individual ballots.

Embedded EVM features such as "electronically limiting the rate of casting votes to five per minute", an electronic database of "voting signatures and thumb impressions" to confirm the identity of the voter.Indian EVMs are stand-alone machines built with once write, read-only memory**.** The EVMs are produced with secure manufacturing practices, and by design, are self-contained, battery-powered and lack any networking capability. They do not have any wireless or wired internet components and interface. During the election period, the citizen's fingerprint is sensed using fingerprint module and it is searched in the data base which is predefined for matching purpose.Next, the QR code scanner is used to scan the Aadhar card of the same citizen. Then the citizen's face is captured by the camera for the future purpose. Then the citizen can vote on the electronic ballot.If unauthenticated citizen give again to

vote then buzzer is activated.This type of system can desing to implimente using raspberry pi,which have many feature.
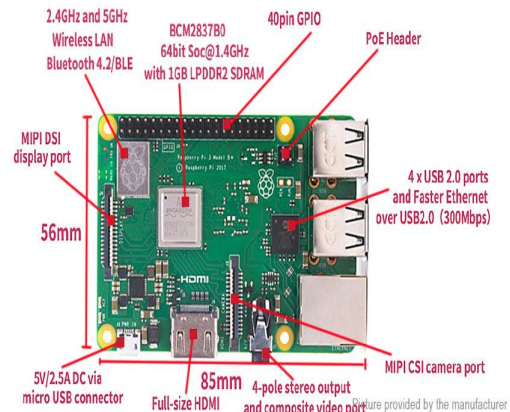

Fig:Raspberry pi B+ board

II. LITERATURE SURVEY

2.1 Smart Voting System

system that gives the provision to vote from anywhere in India so the voter no need to come to his constituency if he is in any other place on the day of voting. We are using aAadhar database where the persons information are stored. This doesn't give any security to casting their vote. It did not provide safty for citizen's database.

2.2AADHAR based Electronic Voting Machine using Arduino

It is not possible for a vote to be altered e laminated the invalid vote cannot be counted from the finally tally. One can change the program installed in the EVM and tamper the results after the polling. The very commonly known problem Rigging which is faced in every electoral procedure.

2.3Aadhaar Based FQ Voting Machine

Now a more Indian citizens are have two voter ID card, so can Give one person give two votes by two voter ID

Card. Mainly used in GSM module, it is easily hacked via IOT. At the time of election, EVM program can changed third party. It needs more mansource during election time.

III. EXISTING VOTING SYSTEM

Electronic voting machines have been in use in India since 1999. Using EVMs means doing away with paper ballots, and in turn, saving millions of trees from being cut. These machines don't require electricity and run on batteries. At the same time, the EVMs are lighter and portable compared to the huge ballot boxes. EVMs or electronic voting machines provide the voter with a button for each choice which is connected by a cable to an electronic ballot box. An indian EVM mainly encompass of two units

1. control unit and
2. balloting unit

2.1.1 Control Unit

The Control Unit controls the polling process. It is operated by the Presiding Officer or the First Polling Officer.

2.1.2 Balloting Unit

The Balloting Unit is that unit of the machine which the voter operates to exercise his / her franchise.

Then the citizen's can authenticated, once authentication process can complited to vote. Unauthorized citizen to enter the finger means SMS send to the control room through GSM module. The main problem in existing system is easily can hack third party. Because, SIM is connected to the network.

IV. PROPOSED SYSTEM

Our proposed approach is very easily understanding to all citizen's. This EVM cannot hack third party. Because,This EVM doesn't connect any network. The proposed system implement to face capturing and store our database for future purpose. The face is captured using normal camera. This process can remodified face recoganition purpose for future. It does not require any manpower at the time of election. Comparing to traditional voting systems electronic voting systems have many benefits such as ensuring better accuracy by eliminating human error, increased speed of computation and lower operating cost through automated means.

4.1 Advantage Of Proposed System

This paper include many advantages with update voting machine. While recent hacks deserve our attention, the overwhelming majority of voting is not done over the internet. Voters should vote early when possible, to avoid potential delays caused by machine breakdowns on Election Day.Based on the promise of greater efficiency, better scalability, faster speed, lower cost and more reliability, voting process is currently shifting from paper based manual process to electronic based voting systems.
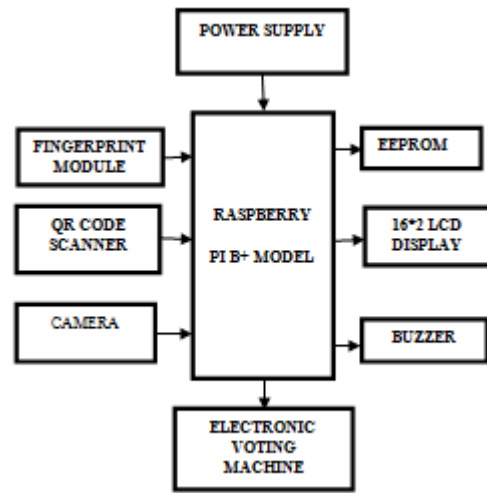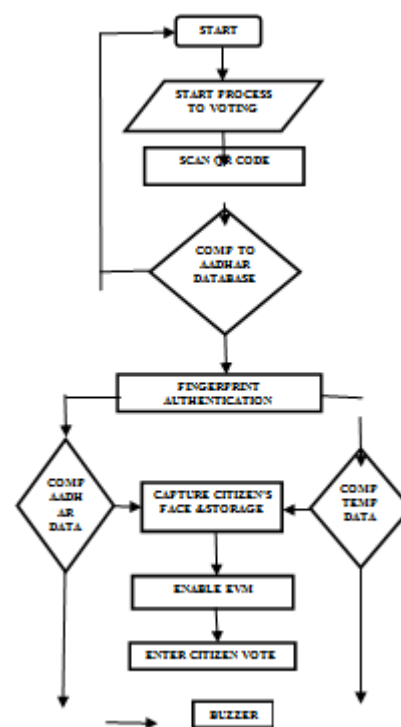
V. BLOCK DIAGRAM

Fig:Block Diagram for FQ Based voting System

VI. FLOW CHART

VII. HARDWARE DESCRIPTION

The are main components of this project is

- Power supply unit
- Raspberry pi B+
- Fingerprint module
- OR code scanner
- Cemara
- 16*2 LCD display unit
- Storage unit
- Buzzer unit

7.1 Power supply unit

Power supply consist of step down transformer(230-(0-12)v),bridge rectifier, filter and voltage regulator(LM7805),which produce output of 5v.

7.2 Raspberry pi B+

The Raspberry Pi 3 Model B is a tiny credit card size computer that was designed in the UK by the Raspberry Pi Foundation. Originally intended to assist in teaching computer science, the Pi's accessible price makes it popular with hobbyists/makers/hackers who use it to create everything from Living Room PCs to Robotics Projects. Just add a keyboard, mouse, display, power supply, micro SD card with installed Linux Distribution and you'll have a fully fledged computer that can run applications from word processors and spreadsheets to games.

As the Raspberry Pi 3 supports HD video, you can even create a media centre with it. The Raspberry Pi 3 Model B is the first Raspberry Pi to be open-source from the get-go, expect it to be the defacto embedded Linux board in all the forums. Here are some of the new Pi's specs:

- Quad core 64-bit processor clocked at 1.4GHz
- 1Gb LPDDR2SRAM
- Bluetooth 4.2/BLE
- Higher speed Ethernet up to 300Mbps
- Power over Ethernet capability(via a separate PoE HAT)

7.3 Fringerprint module

A fingerprint scanner is a type of electronic security system that uses fingerprints for biometric authentication to grant a user access to information or to approve transactions. Human fingerprints are practically unique, which

is why they're successful at identifying individuals. It's not just law enforcement agencies that collect and maintain databases of fingerprints.

Fingerprint scanners work by capturing the pattern of ridges and valleys on a finger. The information is then processed by the device's pattern analysis/matching software, which compares it to the list of registered fingerprints on file. A successful match means that an identity has been verified, thereby granting access. The method of capturing fingerprint data depends on the type of scanner being used:

Fig:finger print module

7.3 OR code scanner

A QR code (short for "quick response" code) is a type of barcode that contains a matrix of dots. All QR codes have a square shape and include three square outlines in the bottom-left, top-left, and top-right corners. These square outlines define the orientation of the code. The dots within the QR code contain format and version information as well as the content itself. QR codes also include a certain level of error correction, defined as L, M, Q, or H. A low amount of error correction (L) allows the QR code to contain more content, while higher error correction (H) makes the code easier to scan.

Fig:QR code

7.4 Cemara

Digital cameras look very much like ordinary film cameras but they work in a completely different way. When you press the button to take a photograph with a digital camera, an aperture opens at the front of the camera and light streams in through the lens. So far, it's just the same as a film

camera. From this point on, however, everything is different. There is no film in a digital camera. Instead, there is a piece of electronic equipment that captures the incoming light rays and turns them into electrical signals. This light detector is one of two types, either a **charge-coupled device (CCD)** or a **CMOS image sensor**.

Fig:cemara

7.5 LCD display

A liquid crystal display or LCD draws its definition from its name itself. It is combination of two states of matter, the solid and the liquid. LCD uses a liquid crystal to produce a visible image. Liquid crystal displays are super-thin technology display screen that are generally used in laptop computer screen, TVs, cell phones and portable video games. LCD's technologies allow displays to be much thinner when compared to cathode ray tube (CRT) technology.

Liquid crystal display is composed of several layers which include two polarized panel filters and electrodes.
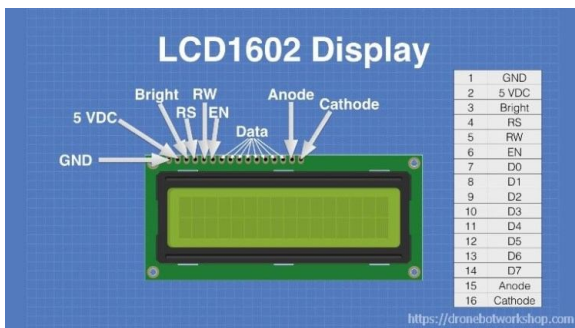

Fig:16*2 LCD display

7.6 Storage unit

EEPROM (electrically erasable programmable read-only memory) is user-modifiable read-only memory (ROM) that can be erased and reprogrammed (written to) repeatedly through the application of higher than normal electrical

voltage. Unlike EPROMchips, EEPROMs do not need to be removed from the computer to be modified. However, an EEPROM chip has to be erased and reprogrammed in its entirety, not selectively. It also has a limited life - that is, the number of times it can be reprogrammed is limited to tens or hundreds of thousands of times. In an EEPROM that is frequently reprogrammed while the computer is in use, the life of the EEPROM can be an important design consideration.

A special form of EEPROM is flash memory, which uses normal PC voltages for erasure and reprogramming.

7.7 Buzzer unit

A buzzer is understood as a device that creates an audible tone under the influence of an applied external voltage. This output may either be in the form of a buzzing or a beeping sound. This is a result of the induced rapid movements created in the diaphragm of the buzzer.

Fig:Buzzer

VIII. CONCULSION

Many election officials look to electronic voting systems as a means for improving their ability to more effectively conduct and administer elections. At the same time, many information technologists and activists have raised important concerns regarding the security of such systems. Policy makers are caught in the midst of a controversy with both political and technological overtones. The public debate about electronic voting is characterized by a great deal of emotion and rhetoric.

Asking the Right Questions About Electronic Voting describes the important questions and issues that election officials, policy makers, and informed citizens should ask about the use of computers and technology in the electoral process--focusing the debate on technical and policy issues that need resolving. The report finds that while electronic voting systems have improved, federal and state governments have not made the commitment necessary for e-voting to be

widely used in future elections. More funding, research, and public education are required if e-voting is to become viable.

This research attempts to incorporate Fast and Accurate Biometric technique into the E-Voting System to prevent an unauthorized person to vote. This work has many advantages over the traditional voting system like reduced polling time, less problems in electoral preparation, strong authentication mechanism, easy and accurate counting, flexibility to voter for vote cast irrespective of geographical location and quick publication of results. This chapter concludes the thesis summarizing main contribution and discusses their extendibility. The proposed model and framework enhances the security issues into the electronic voting system with respect to eliminating bogus voting and vote repetition, less election expenditure, more transparency and fast results. The context and the validity of the problem space are established through a comprehensive review of relevant research and applications of biometric security issues in EVM. This is followed by a brief description on the terminology of biometric security issues in the context of EVM to establish the problem space. In brief, the reliable and security mechanism have been presented in this thesis. Appropriate terminology in the context of biometric security issues has been defined and applied to observe the behavior of EVM in this research work.

REFERENCES

[1] Verma, Arvind (2005). "Policing Elections in India". India Review. 4 (3–4): 354–376. doi:10.1080/14736480500302217.

[2] MadhavanSomanathan (2019). "India's electoral democracy: How EVMs curb electoral fraud". Brookings Institution, Washington DC.

[3] Amanpreetkaur, Yashkalyani, Singh KushagraHarila, Rahul madhesiya, ”Microcontroller Based Voice Activated Mobile Controlled Electronic Voting Machine,” International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2013,pages 1331- 1333

[4] FirasHazzaa, SeifedineKadry,”New System of EVoting Using Fingerprint ,”International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 10, October 2012),pages 355-363.

[5] Himanshu Agarwal, G.N.Pandey, “Online Voting System for India Based on AADHAAR ID”, Eleventh International Conference on ICT and Knowledge Engineering, 2013.

[6] Alaguvel.R and Gnanavel.G,” Offline and Online EVoting System with Embedded Security for Real Time,”International Journal of Engineering Research (ISSN : 2319- 6890) Volume No.2, Issue No.2, April 2013, pages 76- 82.

[7] ShaikMazhar Hussain, ChandrashekarRamaiah, Rolito Asuncion, Shaikh AzeemuddinNizamuddin, Rakesh Veerabhadrappa, An RFID based Smart EVM System for Reducing Electoral Frauds 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) Sep. 7-9, 2016, AIIT, Amity University Uttar Pradesh, Noida, India.

[8] D. Ashok Kumar , T. UmmalSariba Begum , “Electronic Voting Machine – A Review”, Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering, March 2012.

[9] Winder, Davey. "Hackers Claim 'Any' Smartphone Fingerprint Lock Can Be Broken In 20 Minutes".

[10] QR Codes hold up to 2.9 KB whereas the smallest known computer virus is about one-tenth that size "The Smallest Virus I Could Manage”.

[11] Tarui, Yasuo; Hayashi, Yutaka; Nagai, Kiyoko (1971-09-01). "Proposal of electrically reprogrammable non-volatile semiconductor memory". Proceedings of the 3rd Conference on Solid State Devices, Tokyo. The Japan Society of Applied Physics: 155–162.

[12] Simko, Richard T. (17 March 1977). "Electrically programmable and electrically erasable MOS memory cell".