IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

Design and Development of Security Based Electronic Voting Machine Using IOT

M.Shanmugam[1], R.Karthikadevi[2], S.Sandhiya[2], V.Aishwariya[2], T.Ishwarya[2]

Assistant Professor, Department of ECE, Mahendra Engineering College, Mahendhirapuri, Mallasamudram West, Namakkal, Tamil Nadu, India[1]

Department of ECE, Mahendra Engineering College, Mahendhirapuri, Mallasamudram West, Namakkal, Tamil Nadu, India[2]

ABSTRACT: Voting is an integral part of a democratic society. It is a decision making mechanism and security plays an important role in voting. In order to ensure high security, voting machine should be designed and developed with great care. According to Election authorities of India, paperless electronic voting systems are suffering from much vulnerability. By accessing the machines Election insiders and fraudsters are altering the election results. There is a need of voting system which is robust and secure. Here, an idea is proposed to upgrade the present voting system that is based on biometric traits (Iris, Fingerprint) of voter which are saved in a government database. The principle used in EVM is Internet of Things. The principle used is 'IMAGE PROCESSING' (converting a image into a digital format-biometric).

I. INTRODUCTION

Voting is the most pivotal process which is carried out to reveal the opinion of the people in selecting government and in any issue that is under consideration. So the conventional voting systems based on paper voting are being replaced by electronic voting machines. Voting is a decision making mechanism in the society and security is indeed an essential part of voting. The term "electronic voting" represents the practice of electronic means in voting to safeguard the security, reliability, and transparency. The crucial role in determining the result of an election, electronic voting systems should be developed with the greatest responsibility and security. Electronic voting machines aid blind users by reading off the instructions using headphones and also provide essential tools to help people with disabilities. Voting machines are the combination of mechanical and electronic equipment's which are needed for casting votes and displaying the election results. The main proposal for using the voting machines was given in 1838.There are large numbers of smart systems present which employ microcontrollers for their operation and several other voting systems have been developed for ensuring a secured vote casting process. The design presented in incorporates voter information facility for getting the information about the number of voters at a place. In this paper, Wi-Fi based design of an electronic voting machine has been presented for sending the polling results to a monitoring station via mobile network and PC. This system is fully secured and chances of digital tampering are also avoided and turbidity sensors are used. Raspberry PI receives data from Arduino this objective of the project is to very useful of the election commission in design and development security used voting for government using IoT.

The Election Commission of India developed the country's EVMs in partnership with two government-owned companies, the Electronics Corporation of India limited (ECIL) and Bharat Electronics Limited (BEL).Though these companies are owned by the Indian government, they are not under the administrative control of the Election Commission. They are profit-seeking vendors that are attempting to market EVMs globally.

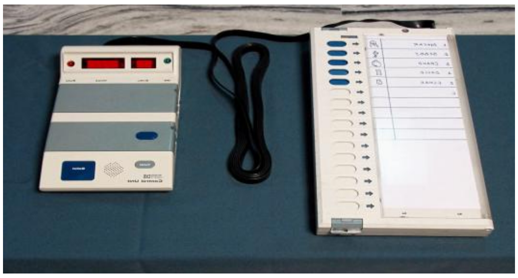


Fig 1: SEPARATE CONTROL AND BALLOT

The Indian EVMs were developed inside the first Nineteen Eighties by ECIL. They were utilized in certain parts of the country, but were never adopted nationwide. They introduced the planning of system accustomed this gift day (see Figure 1), along with the separate management and ballot units and additionally the layout of every parts. Thesefirst-generation EVMs were supported Hitachi 6305 microcontrollers and used code confine external UV-erasable PROMs along with 64kb EEPROMs for storing votes. Second-generation

Models were introduced in 2000 by every ECIL and BEL. These machines affected the code into the CPU and upgraded various parts. They were step by step deployed in larger numbers and used nationwide beginning in 2004.In 2006, the manufacturers adopted a third-generation vogue incorporating additional changes suggested by the commission. In step with commission statistics, there are one, 378,352 EVMs in use in Gregorian calendar month 2009. Of these, 448,000 were third-generation machines factory-made from 2006 to 2009, with 253,400 from BEL and 194,600 from ECIL. The remaining 930,352 were the second-generation models factory-made from 2000 to 2005, with 440,146 from BEL and 490,206 from ECIL. (The initial generation machines area unit deemed too risky to use in national elections as a results of their 15-year service life has terminated , though they are apparently still utilized in certain state and native contests.) Inside the 2009 parliamentary election, there are 417,156,494 votes solid, for a mean of 302 votes per machine. The EVM we've got a bent to test is from the foremost vital cluster, a second generation ECIL model. It is a true machine that was factory-made in 2003, and it has been utilized in national elections. It had been provided by a offer international organization agency has requested to remain anonymous. Photos of the machine and its inner operative. Tally Votes, The EVM records votes in its internal memory. At a public tally session, employees remove a seal on the management unit and press the result I button (left) to reveal the results. The machine consecutive outputs the number of votes received by each candidate using a bank of 7-segment LEDs (right). Here, candidate selection 01 has received seven votes. Pear throughout this paper. Various kinds and generations of machines have certain variations, but their overall operation is improbably similar. We've got a bent to believe that just about all of our security analysis is applicable to all or any or any EVMs presently utilized in state.

Elections in state area unit conducted nearly utterly mistreatment electronic choose machines developed over the past twenty years by a mix of government-owned companies. These devices, noted in state as EVMs, are praised for his or her simple vogue, easy use, and responsibility, but recently they have put together been criticized following widespread reports of election irregularities. Despite this criticism, many details of the machines' vogue haven't been publicly disclosed, which they haven't been subjected to a rigorous, freelance security analysis.In this paper, we have a tendency to gift a security associatealysis of a true Indian EVM obtained from an anonymous supply. We have a tendency to describe the machine's style and operation intimately, and that we appraise its security in light-weight of relevant election procedures. We have a tendency to conclude that in spite of the machines' simplicity and smallest software package trustworthy computing base, they're vulnerable to serious attacks that may alter election results and violate the secrecy of the ballot. We have a tendency to demonstrate 2 at-tacks, enforced victimization custom hardware, That can be distributed by dishonest election insiders or alternative criminals with solely temporary physical access to the machines. This case study carries vital lessons for Indian elections and for electronic vote security additional usually.

The legal system of a rustic consists of bound laws that outline however the preference of individuals is collected and the way outcome of the polling method is indicating the desire of individuals. To implement such a system within the largest democracy within the world could be a cumbersome task. Associate autochthonous Electronic mechanical device was introduced by the committee of Bharat to beat the problems with manual vote that was slower and inefficient. During this paper the Indian Electronic vote Machine's Protocol for vote is enforced on a field programmable gate array. The ASIC based mostly} style is understood to be quicker than a microcontroller based style. {Furthermoreover what is additional} the utilization of associate ASIC based mostly style can create the Electronic mechanical device a more reliable and tamper resistant machine. The new Voter-verified paper audit path (VVPAT) system might even be interfaced with the ASIC based mostly style. The protocol of Indian Electronic mechanical device has been with success enforced on a Basis a pair of board victimization Verilog high-density lipoprotein. The FPGA based mostly} implementation gets [*fr1] the task finished ASIC based EVM.

II. METHOD

PROPOSED BLOCK DIAGRAM:

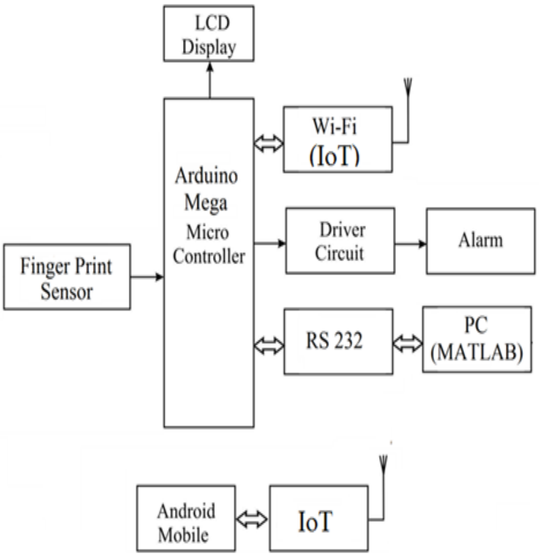


Fig 2: BLOCK DIAGRAMDESIGN AND DEVELOPMENT OF SECURITY BASED ELECTRONIC VOTING MACHINE USING IoT

FINGER PRINT SENSOR

The fingerprint device transforms the fingerprint info of a finger beneath investigation into an electrical signal. The device incorporates a contact device or device plate of a electricity material. This device plate incorporates a contact surface. The finger exercises a contact pressure on that and changes thereby the distribution of electrical charges on the contact surface. The new charge distribution is in accordance with the fingerprint pattern of the finger. The device additional incorporates an electrical device that provides the electrical signal in accordance with the distribution of charges.

Fig 3: FINGERPRINT SENSOR.

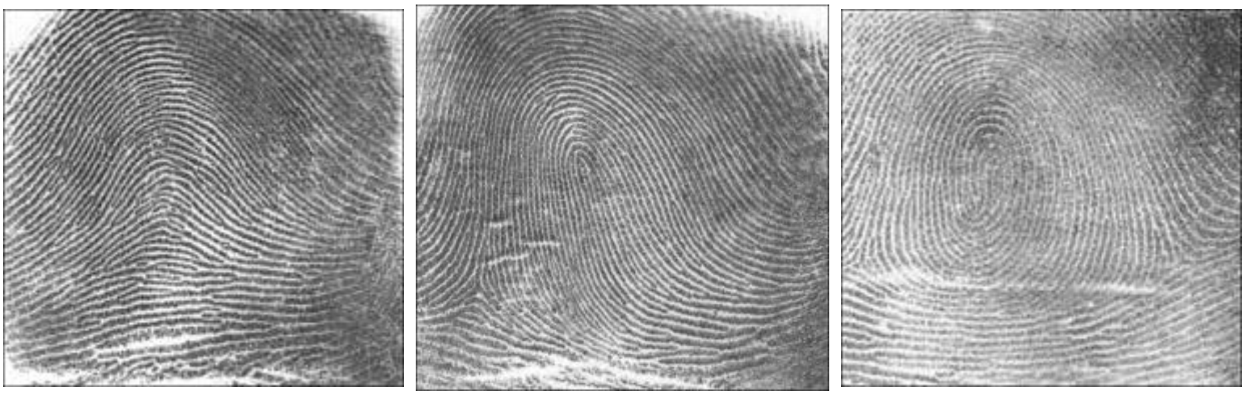
According to this invention, a fingerprint sensing element for reworking the fingerprint data of a contacting finger into an electrical signaling incorporates a detector or a contact device that is formed of an electricity material. The contact device has a minimum of 2 surfaces. One in every of these surfaces may be a contact surface for work out a contact pressure on it by suggests that of the contact finger underneath investigation. Because of the contact pressure, the density of the electrical charges on the surfaces are modified in keeping with the fingerprint pattern of the contact finger.

The fingerprint device any contains an electrical device for determinant the distribution of charges of a minimum of one in every of the mentioned surfaces. It provides the electrical output in accordance with the distribution of the electrical charges.

In this fingerprint sensor, the information of the fingerprint is directly transformed from mechanical information (impression on the contact device) into electric information (output signal of the electric device.)

The contact device is ideally made from a versatile electricity compound. It may also be made from a electricity ceramic. If a compound is employed, ideally the well-known electricity compound polyvinylidene halide (PVDF) or a connected material will be applied. If a ceramic is employed, a lead zirconate titinate ceramic will be applied, as an example containing atomic number 56 titinate or triglycine salt. The electricity material could also be structured, that includes associate array of a matrix of pixels, so as to avoid interference between adjacent valleys of the fingerprint. The segmentation could also be identical or not.

The 3 basic patterns of fingerprint ridges area unit the arch, loop, and whorl. Associate arch may be a pattern wherever the ridges enter from one facet of the finger, rise within the center forming associate arc, then exit the opposite facet of the finger. The loop may be a pattern wherever the ridges enter from one facet of a finger, type a curve, and have a tendency to exit from identical facet they enter. Within the whorl pattern, ridges type circularly around a central purpose on the finger. Scientists have found that members of the family usually share identical general fingerprint patterns, resulting in the idea that these patterns area unit transmitted.

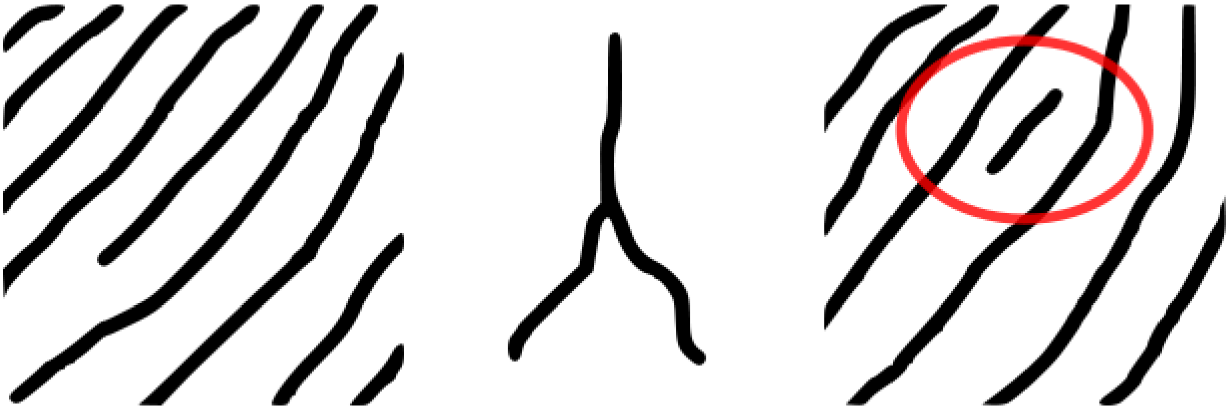


The arch pattern. The loop pattern. The whorl pattern.

Fig 4: FINGER PRINT PATTERNS

MINUTIA FEATURES

The major item options of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot). The ridge ending is that the purpose at that a ridge terminates. Bifurcations are points at that one ridge splits into 2 ridges. Short ridges (or dots) are ridges that are considerably shorter than the typical ridge length on the fingerprint. Trivialities and patterns are vital within the analysis of fingerprints since no 2 fingers are shown to be identical.



Ridge ending. **Bifurcation.** **Short Ridge (Dot).**

Fig 5: MINUTIA FEATURES

FINGERPRINT SENSORS

A fingerprint detector is Associate in nursing device accustomed capture a digital image of the fingerprint pattern. The captured image is termed a live scan. This live scan is digitally processed to form a biometric template (a assortment of extracted features) that is keep and used for matching. This can be an outline of a number of the additional normally used fingerprint detector technologies..

OPTICAL

Optical fingerprint imaging involves capturing a digital image of the print victimization actinic radiation. This kind of detector is, in essence, a specialized camera. The highest layer of the detector, wherever the finger is placed, is thought because the bit surface. At a lower place this layer may be a light-emitting phosphor layer that illuminates the surface of the finger.

The light mirrored from the finger passes through the phosphor layer to AN array of solid state pixels (a charge-coupled device) that captures a visible image of the fingerprint. A damaged or dirty bit surface will cause a foul image of the fingerprint. An obstacle of this kind of detector is that the undeniable fact that the imaging capabilities square measure plagued by the standard of skin on the finger. For example, a grimy or marked finger is troublesome to image properly. Also, it's potential for a personal to erode the outer layer of skin on the fingertips to the purpose wherever the fingerprint isn't any longer visible. It can even be simply fooled by a picture of a fingerprint if not to mention a "live finger" detector. However, in contrast to electrical phenomenon sensors, this detector technology isn't liable to static discharge injury.

III. CONCLUSION

Optical fingerprint imaging involves capturing a digital image of the print victimization actinic radiation. This kind of detector is, in essence, a specialized camera. The highest layer of the detector, wherever the finger is placed, is thought because the bit surface. At a lower place this layer may be a light-emitting phosphor layer that illuminates the surface of the finger.

The light mirrored from the finger passes through the phosphor layer to AN array of solid state pixels (a charge-coupled device) that captures a visible image of the fingerprint. A damaged or dirty bit surface will cause a foul image of the fingerprint. An obstacle of this kind of detector is that the undeniable fact that the imaging capabilities square measure plagued by the standard of skin on the finger. For example, a grimy or marked finger is troublesome to image properly. Also, it's potential for a personal to erode the outer layer of skin on the fingertips to the purpose wherever the fingerprint isn't any longer visible. It can even be simply fooled by a picture of a fingerprint if not to mention a "live finger" detector. However, in contrast to electrical phenomenon sensors, this detector technology isn't liable to static discharge injury.

REFERENCES

1. “Analysis and Management of the Impacts of a High Penetration of Photovoltaic Systems in an Electricity Distribution Network”, S. J. Lewis.
2. “Security Analysis of India’s Electronic Voting Machines” Scott Wolchok, Eric Wustrow, J. Alex Halderman (Jan 2019).
3. “Prototyping of Indian Electronic Voting Machine” Tushar Puri, Jaspreet Singh, Hemant Kaushal International Journal of Engineering Research and Development (May 2017).
4. “Secret Suffrage in Remote Electronic Voting Systems” Adri Rodríguez-Pérez (2017).
5. “Election Voting Machine - A Review Sanket M. Gawade, Ninad S. Mandavkar, Sanket S. Mane, Chinmayee N. Manjarekar” International Journal of Engineering Trends and Technology (IJETT) –(Aug 2017).
6. “Verifiable Classroom Voting in Practice”FengHao, Dylan Clarke, and Brian Randell (2017).

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details