International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 5, July-August 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Experimental Approach to IoT Based Secure Online Voting System using Raspberry PI & Extended Facilities with Arduino UNO

Ashok P. Mane[1], Vimokshavardhan. A. Daware[2]

[1]Assistant Professor & Head, [2]Assistant Professor,
[1,2]E & TC Department, TPCT"s College of Engineering, Osmanabad, Maharashtra, India

ABSTRACT

Electronic voting machine has developed and used in many countries all over world, India is one of them who has world's largest democracy. Some politician takes advantage of electronic voting machine to submit vote on behalf of absent people or died peoples. This is the most important and controversial topic in India. Most of the people doesn't have a faith on EVM machine and Opponent parties in India still having issue with EVM. Recently in India during Loksabha election 2019 election commission of India started using VVPAT to synchronize votes. But still some opponents have doubt on Electronic voting machine and VVPAT too. So all opponent parties are requesting to conduct a election on ballot paper which is easy to vote but hard to count and time consuming system. Hence we try to overcome some disadvantage of EVM by introducing Advance Electronic voting machine to avoid bogus and fake voting. This advance Electronic voting machine is IoT(Internet of Things) based machine which is directly linked with Governments servers to access and compare voters valid data. This project is designed for integrating Electronic Voting Machine with the data of the voter as in the Aadhar.

KEYWORDS: *Aadhar, EVM, IoT, VVPAT, Raspberry Pi, Fingerprint Sensor*

How to cite this paper: Ashok P. Mane | Vimokshavardhan. A. Daware "Experimental Approach to IoT Based Secure Online Voting System using Raspberry PI & Extended Facilities with Arduino UNO" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-5, August 2020, pp.1038-1041, URL: www.ijtsrd.com/papers/ijtsrd33068.pdf

IJTSRD33068

I. INTRODUCTION

In any democracy trust can be gained through a transparent voting system only. In India Aadhar card is primary identity of each and every Indian. Aadhar card is also linked with different kind of identity proofs like PAN card. Electronic voting machine has been a very important and controversial topic ever since the loksabha election 2019. So many expert expressed their negative opinion on electronic voting machine basically electronic voting is an system were voters are cast their vote which collected automatically.EVM can record a maximum of 3840 votes and can cater to maximum of 64 candidates. The election commission of India is very proud of this system and stated that the machines are perfect and tamperproof. Still some opponent parties have allegations on EVM.

Hence we are going take advantage of Aadhar card for transparent voting system so in this project we have proposed a system to stop bogus and fake voting by interfacing finger print scanner recognition system using Raspberry Pi 3 Model B. The finger print recognition and Aadhar card details gets verified with government servers data if the information is valid the controller send valid message on screen. Due to this system result are seen in which the total votes obtained by each party for all word combined is calculated automatically. Hence the result can be announced immediately and correctly without malpractice.

II. MOTIVATION

Motivation comes from politician take advantage of electronic voting machine to submit vote on behalf of absent people or died people. Recently in India during loksabha election 2019 election commission of India started using VVPAT to synchronize votes. But still some opponents have doubt on Electronic voting machine and VVPAT too. So all opponent parties are requesting to conduct an election on ballot paper which is easy to vote but hard to count and time consuming system. Hence we try to overcome some disadvantage of EVM by introducing Advance Electronic voting machine to avoid bogus and fake voting.

III. LIMITATIONS OF CURRENT SYSTEM

1. Recent elections in US many software programmers have claimed that EVMs are vulnerable to malicious.
2. Corrupted officers may tamper with the EVM.
3. Some physically challenged people have complained that touch base screen is not efficient to capture vote perfectly. Sometimes it leads to voter ending up voting for someone else.

IV. BLOCK DIAGRAM OF THE SYSTEM

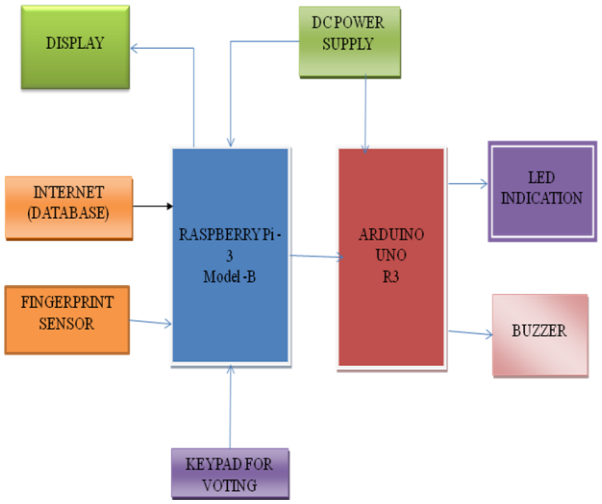

Fig.1 Block Diagram

V. EXPLAINATION OF BLOCK DIAGRAM

1. Raspberry Pi 3 Model B

Following are the main Specification of Raspberry Pi 3: Chipset: Broadcom BCM2837, CPU: 1.2GHz quad-core 64-bit ARM cortex A53

Ethernet: 10/100, USB: Four USB 2.0 with 480Mbps data transfer, Storage: Micro SD card or via USB-attached storage, Wireless: 802.11n Wireless LAN (Peak transmit/receive throughput of 150Mbps), Bluetooth 4.1, Graphics: 400MHz Video Core IV multimedia, Memory: 1GB LPDDR2-900 SDRAM, Expandability: 40 general purpose input-output pins.

Fig.2 Raspberry Pi 3 Model B

2. Microcontroller (ARDUINO UNO R3)

Following are the main Specification of Micro Controller ATMEGA 328:
ATmega328 is an 8-bit and 28 Pins AVR Microcontroller, manufactured by Microchip, follows RISC Architecture and has a flash type program memory of 32KB.

It has an EEPROM memory of 1KB and its SRAM memory is of 2KB.

It has 8 Pin for ADC operations, which all combines to form Port A(PA0 – PA7).

It also has 3 built in Timers; two of them are 8 Bit timers while the third one is 16-Bit Timer. Arduino UNO is based on atmega328 Microcontroller. It's UNO's heart.

It operates ranging from 3.3V to 5.5V but normally we use 5V as a standard.

3. Bluetooth Device HC-05

Following are the main Specification of Bluetooth Device HC-05:
Slave default Baud rate: 9600, Data bits:8, Stop bit:1,Parity:No parity.Auto-connect to the last device on power as default. Permit pairing device to connect as default.

4. Fingerprint Scanner R305:

Following are the main Specification of Fingerprint Scanner R305: Supply voltage: DC 4.2 ~ 6.0V. Supply current: Working current: 50mA (typical) Peak current: 80mA Fingerprint image input time: <0.3 seconds. Window area: 14x18 mm, Matching method: Comparison method (1: 1).

Fingerprint identification is an active research area nowadays. An important component in fingerprint identification systems is the fingerprint matching algorithm. According to the problem domain, fingerprint matching algorithms are classified in two categories: fingerprint verification algorithms and fingerprint identification algorithms. The aim of fingerprint verification algorithms is to determine whether two fingerprints come from the same finger or not. On the other hand, the fingerprint identification algorithms search a query fingerprint in a database looking for the fingerprints coming from the same finger. Despite the widespread use of fingerprints, there is little statistical theory on the uniqueness of fingerprint minutiae. A critical step in studying the statistics of fingerprint minutiae is to reliably extract minutiae from the fingerprint images. However, fingerprint images are rarely of perfect quality. They may be degraded and corrupted due to variations in skin and impression conditions. Thus, image enhancement techniques are employed prior to minutiae extraction to obtain a more reliable estimation of minutiae locations.

Fig.3 Basic of fingerprint

A fingerprint is consists of ridges and valleys. The ridges are the black area of the fingerprint and the valleys are the white area that exists between the ridges. Many classifications are given to patterns that can arise in the ridges and some examples are given in the figure above. The most commonly used part in current fingerprint identification technologies are ridge endings because they can be easily observed by only seeing at points that surrounds.

VI. IMPLEMENTATION RESULTS

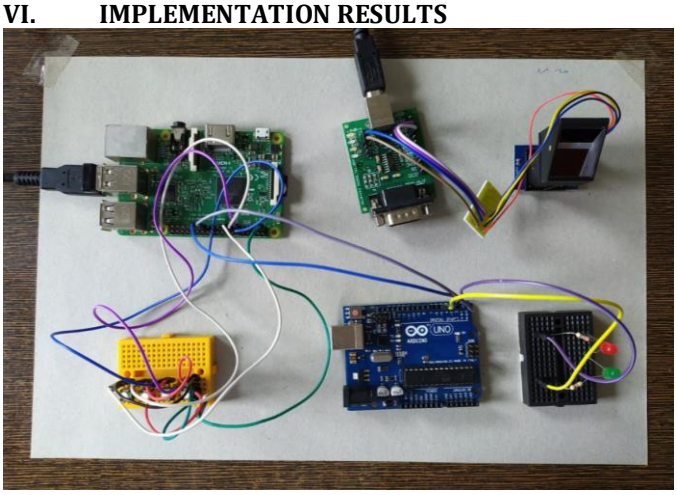

Fig4. Experimental Set up of the System

Steps to follow by the voter at the time of voting:-

1. Please Enter Your Fingerprint.
2. Sensor will read the Thumb Impression if it is matched then go to step 3.If not matched then message will be displayed please register your details.
3. If Voter Registered; then message will be displayed as Match Found with User No.--
4. User Fingerprint Identified. Please Press A switch for voting.
5. After pressing any one of the switch message will be displayed as You voted Candidate No.---
6. Now System ready for the next voter follow the steps from step no.1 to step no. 5

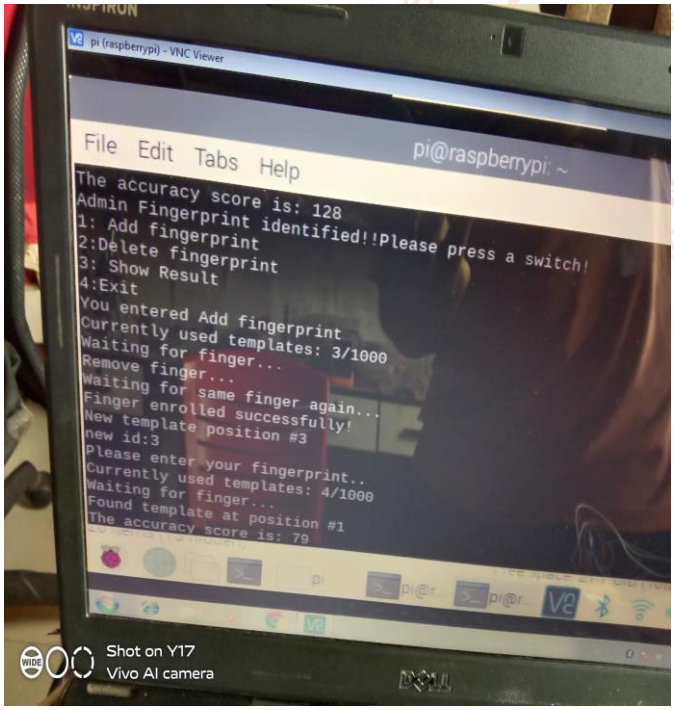

Fig.5. Display shows the Admin Enrolls the voter before voting.

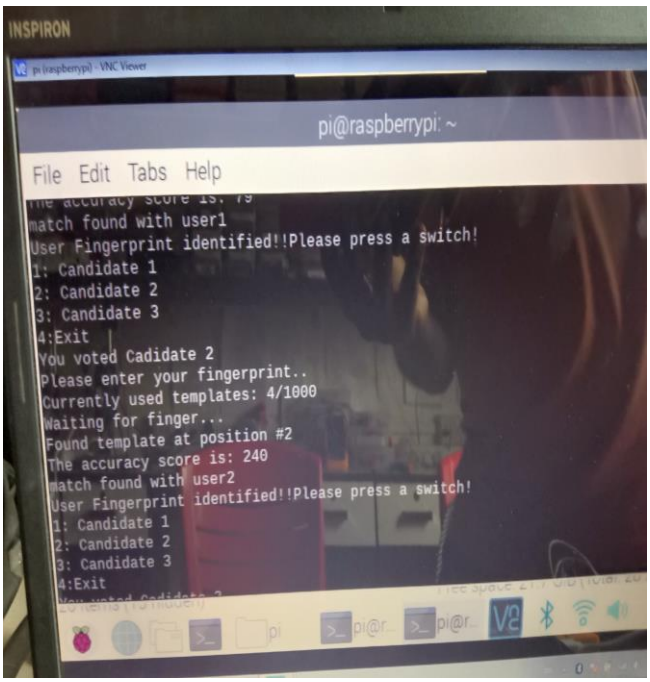

Fig.5. Display shows the voting done by the vote

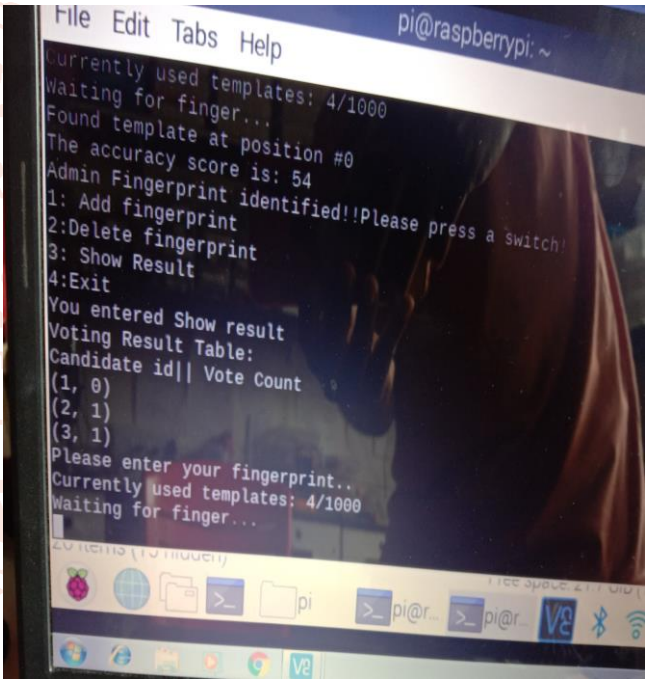

Fig.7. Display shows the voting result after completion of voting. (Admin Mode)

VII. CONCLUSION

Fingerprints considered as one of the most popular biometric methods used for human recognition. Every person in the globe is born with unique fingerprint even twins born with totally different fingerprints and fingerprint is naturally unchangeable throughout life. For that reason fingerprint voting system has been made and the person ID has been replaced with his fingerprint with QR scan. This paper suggest that the EVM system has to be further studied and improved to reach all the levels of community, so that the voter's trust on the election process will increase and election officials will make more involvement in purchasing the innovated EVM's for conduct efficient, secure, corruption free Elections.

REFERENCES

[1] P. Tamilarasu, S. Aadhithyan, K. Gowthaman, V. Hariprakash "Fingerprint based Electronic Voting Machine" IJCESR, Vol. 5, Issue 2, ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, 2018.

[2] Rahul Dongre, Pankaj Jhare , Shubham Pal, Sangeeta Dhurve, Naina Suryawansi, Krunal Itankar "A Review Paper on Fingerprint Based Voting Machine" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 6 Issue 4, ISSN (Print) : 2320 – 3765 ISSN (Online): 2278 – 8875, April 2017.

[3] Yurong Yao, Lisa Murphy "Remote electronic voting systems: an exploration of voters perceptions and intention to use" European Journal of Information Systems Volume 16, Issue 2, pp 106–120, April 2007.

[4] Vishal Vilas Natu "Smart-Voting using Biometric "International Journal of Emerging Technology and Advanced Engineering", Volume 4,Issue 6, June 2014.

[5] D. Ashok Kumar, T. Ummal Sariba Begum, "A Novel design of Electronic Voting System Using Fingerprint," International Journal of innovative technology & creative engineering, vol.1 Issue 1, pages 12-19, January 2011.

[6] P. Anial, K. Rajasekhar, K. Ravikumar, T. Phanisiva Shankar "Touch Screen Based Electronic Voting System", international journal of Engineering Research and Technology,Vol.1, Issue 7, September-2012.

[7] Firas Hazzaa, Seifedine Kadry, "New System of E-Voting Using Fingerprint", International Journal of Emerging Technology and Advanced Engineering, Vol. 2, Issue 10, pages 355-363, October 2012.

[8] A. Piratheepan, S. Sasikaran, P. Thanushkanth, S. Tharsika, M. Nathiya, C. Sivakaran, N. Thiruchchelvan and K. Thiruthanigesan "Fingerprint Voting System Using Arduino" Middle-East Journal of Scientific Research ISSN 1990-9233, pp 1793-1802, 2017.

[9] Daware Vimokshavardhan A, Mane Ashok P "Secure Online system" IJSART Volume 5 Issue 11 November 2019 ISSN (online) 2395-1052 Pages 107 – 109.