IOT based Voting using Fingerprints: Analysis

[1]Anujsingh R. Bais, [2]H.K. Bhangale
[1]Student, [2]Head of Department
[1]ME (Digital Electronics),
[1]GHRIEM, Jalgaon, India

Abstract: Elections. A procedure where eligible candidate(s) contest with each other for ruling over a province in a village, district, state or even nation. The contest has to be fair and square and for this, a rigid process called 'voting' is held where people cast their votes i.e. select the candidate whom they think is capable of doing a firm work for them and bringing their expectations into reality. Voting is not a modern thing. It dates back in old times where people used to cast votes by writing the names of the candidates on a paper and drop it in boxes, later called as 'ballot box'. Then EVM (Electronic Voting Machines) were introduced. This is too now a part of controversy as it is digital and can be hacked or programmed as needed. But now with use of human biometrics, some of these drawbacks are to be rectified and removed. There comes a new era of 'online voting' which is the need of the hour and which has to be carried out with specific hardwares such as Arduino, which is compact and dynamic.

***IndexTerms* - Arduino, EVM, Online voting.**

I. INTRODUCTION

Before the introduction of EVM in the voting world, Ballot boxes, punch cards, lever pulling, or even just raise of hands would define the results.

1. Ballot Box

- Used before the dawn of this millennium.
- Voters would cast their votes by naming the candidate or just by stamping it on a paper and submitting it in a box.
- Later, counting would be done by appointed government servicemen, which would declare the result.

➢ Drawbacks

1. Too much use of paper.

There was only one provision that each voter shall get a piece of paper and he/she shall have to stamp it or write the name of the candidate over it. Hence a lot of paper shall go to waste.

2. Easily changeable.

The ballot box could be easily changed and stacked with the desired votes pretty easily.

3. Hectic and lengthy procedure.

Every vote was to be counted. Means every piece of paper was to be checked and verified. Sometimes extra votes would be casted illegally and no one could know about it.

2. Lever Pulling

- A lever was used to pull, which was against the name of a certain candidate, and pulling it means that the vote is casted to that candidate.
- Counting would be done by checking how many times the lever was pulled, displayed by the analog counter next to it.

➢ Drawbacks

1. Mechanical failures

Improper use of the lever would cause the lever to get loosen up. Hence the vote may not be casted even the lever was pulled correctly.

2. Would need more maintenance.

The lever pulling mechanism was simple but every voter would use their strengths on a different level, causing the damage.

3. Improper pulling would mean zero or sometimes multiple votes casted.

As discussed earlier, the improper pulling would damage the mechanism and cause votes to get affected.

3. Punch cards

- US used this method to a lot extent in the post cold war era.
- A card was to be punched in a certain row(s) or column(s) such that it will cast vote to a certain candidate.

➢ Drawbacks

1. Improper punching means vote goes to waste.

There used to be a pattern to be punched upon the card and if that is not followed, or goes wrong, then the vote shall go to a wrong candidate or may even get barred.

Then the EVMs were introduced. EVM or 'Electronic Voting Machine' proved to be a new era of voting. The salient features of this system were:-

- A 6V alkaline battery for areas where power was an issue.
- One press, one vote. Once the light blinked and the 'beep' was heard, attempting to cast another vote would be futile.
- Tampering with the EVM would cause it to reset, and all votes getting deleted, this gave a side of security to the voting.
- The EVM was laced with 8051/8085 (Earlier versions). They had stuck with a memory that would save 3840 votes across 64 candidates.

➢ Drawbacks

1. No remote voting possible.

A person coming from a particular area of a constituency, would have to vote in the given voting center of that constituency itself.

2. Fake voting still remains an issue here.

In all of the above methods, authenticity was an issue. Discussing about the present EVM technology, then ID produced can be stated fake or illegitimate. This could cause fake voting and hence a rigged result is on the cards.

Using IOT based voting and biometrics:-

Authenticity is a much needed part of voting and in pursuit of it, the uniqueness which every human posses came into research and hence then, authentication of every human using their fingerprints, iris, DNA, voice and speech recognition came into existence. When every human is registered for his/her ID, they are to be authenticated using any of the above biometrics, which later shall be revivified during the time of voting via the database where the data related to each voter is kept secured under servers. The emphasis of this system is to have 100% authenticity against the voters, causing negligible fake voting or multiple voting.

II. METHODOLOGY

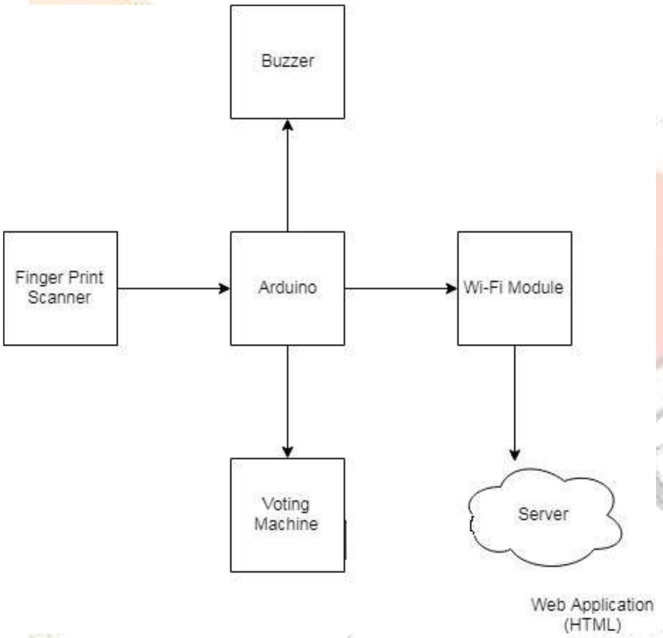


Fig.1 Block Diagram

The block diagram (Fig.1) of proposed system consists of FPS (Finger Print Scanner), Arduino UNO as the main CPU of the system, ESP8266 as a handshake device for the UNO and Wi-Fi module, Buzzer for stating whether the voter has casted its vote or has earlier voted. The EVM which is connected to the Arduino UNO and the votes and its status is then forwarded to the Wi-Fi module from there it goes to server.

2.1 Detailed Description of block diagram:-

Arduino UNO works as the CPU in the system. It has been connected to all the important parts of the system. It runs on 7-12V DC and has a limit of 5-20V. The Fingerprint scanner, which is UART based, capture the images of the fingerprints and then forwards it to UNO. The image of fingerprint is processed and forwarded to the centralized database i.e. Servers, where the match of the fingerprint is to be found. Upon finding it, the buzzer shall beep for a short period, stating that the fingerprint is legitimate and registered and the voter is authentic and eligible to vote. The whole process of sending the scanned fingerprint and then obtaining the acknowledged signal is carried via Wi-Fi. For this, the connectivity needs to be on and running. If the fingerprint of the voter does not match, a message shall be displayed as fingerprint unidentified and when the voter is identified as voted earlier, another message as already voted shall be displayed. But when the voter is authentic and votes for the first time, the regular process of EVM will happen and his/her vote shall be casted.

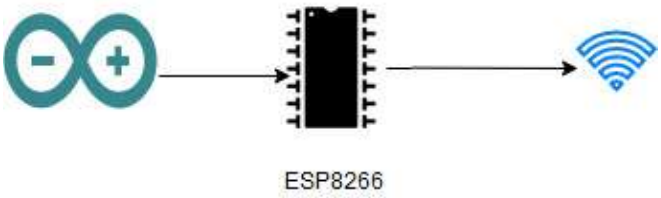


Fig.2 Arduino-Wifi Interfacing using ESP8266

A web application is to be made to make things happen in this system. It will be more of a centralized database where the data related to all the candidates shall be stored. The application shall keep the record of all candidates who have registered to vote, their biometrics, and the votes casted to which candidate etc.

2.2 Arduino UNO

Arduino UNO is a UNO board based on the ATmega328P. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the UNO; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

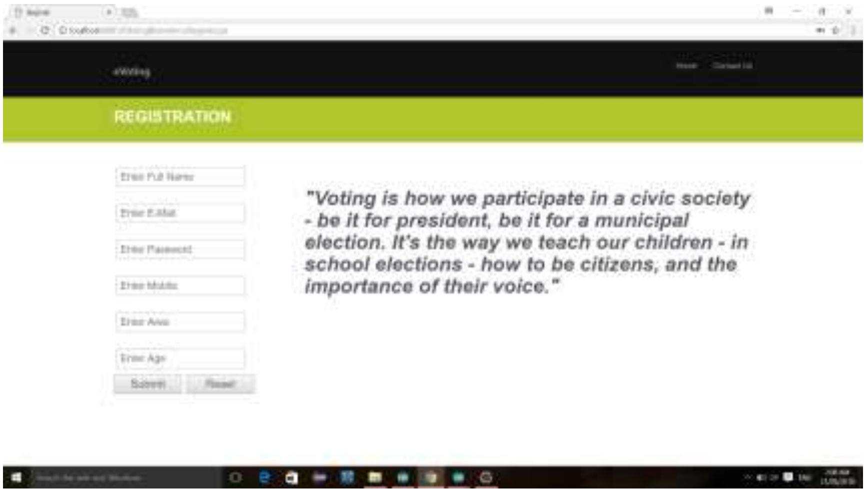
The Arduino family runs upon ATMega 328 technology. Six of the input/output pins can be used as PWM outputs. It has a RISC based architecture with 131 powerful instructions, most of which execute in a single clock cycle. Additionally, it has 32 Kbytes of In-system self-programmable Flash program memory, 1 Kbytes EEPROM and 2Kbytes Internal SRAM. It has output voltage of 5V, Input voltage of 7-12V, Input Voltage limit is 5-20V, DC current per I/O pin is 20mA, DC current for 3.3v pin is 50mA, Even the flash memory is 32kB (ATMega), 0.5kB is used by the bootloader.

Atmega328p is an 8 bit, 28 pin UNO belonging to the AVR family. It has 23 digital input/output pins and 6 analog inputs.

Fig.3 Arduino UNO

2.3 HTML Webpage

A webpage is necessary in this system as it will display the current status of the ongoing voting or even the results. The webpage shall be as a viewer only for the admin. The admin shall have full control of the webpage and it shall be secured using OOP (Object Oriented Programming) which is discussed later. The details of the voter will be stored as soon as they registered themselves. After that, whenever they come to vote, their vote shall be casted as their fingerprint will authenticate their identity



eVoting

Home Contact Us

REGISTRATION

Enter Full Name

Enter E-Mail

Enter Password

Enter Mobile

Enter Area

Enter Age

Submit Reset

"Voting is how we participate in a civic society - be it for president, be it for a municipal election. It's the way we teach our children - in school elections - how to be citizens, and the importance of their voice."

Fig.4 A Snapshot of HTML Webpage dedicated to IOT based voting

.

2.4 Fingerprint scanner

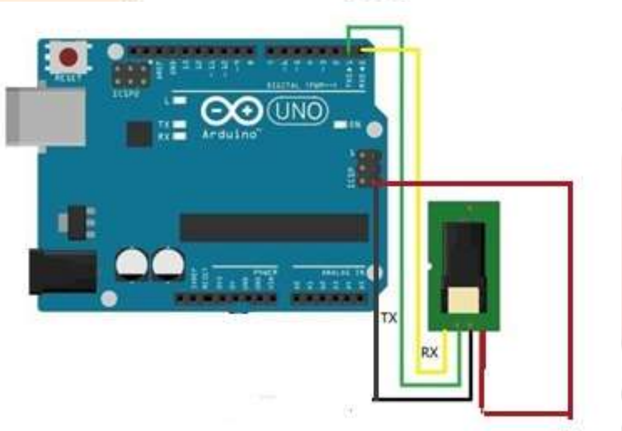


Fig.5 Arduino UNO interfaced with FPS

Fingerprint scanners are of many different methods viz Optical, Capacitive, Ultrasonic etc. In case of optical scanner, this technique relies on capturing an optical image, which is a photograph, and using algorithms that detect unique patterns on the surface, such as ridges or valleys, by analyzing the lightest and darkest areas of the image. these sensors can have a fine resolution, and the better the resolution, the finer details the sensor can get about your finger, increasing the level of security. However, these sensors capture much higher contrast images than a regular camera. These scanners typically have a very high number of diodes per inch to capture these details that close. Of course, it’s quite dark when the finger is placed over the scanner, so optical scanners also incorporate arrays of LEDs as a flash to light up the picture come scan time.

Optical fingerprint imaging involves capturing a digital image of the print using visible light rays. In this type of sensor is depended on a uniquely designed digital camera. Where top layer of the sensor are used to place the finger which is known as the ‘touch surface’. Down of this layer is a light emitting phosphor layer which lightens up the surface of the finger. Then the light is reflected from the finger passes through the phosphor layer to an array of solid state pixels (a charge coupled device) which captures a visual image of the fingerprint which is used for authentication. But a scratched or dirty touch surface can cause a bad image of the fingerprint

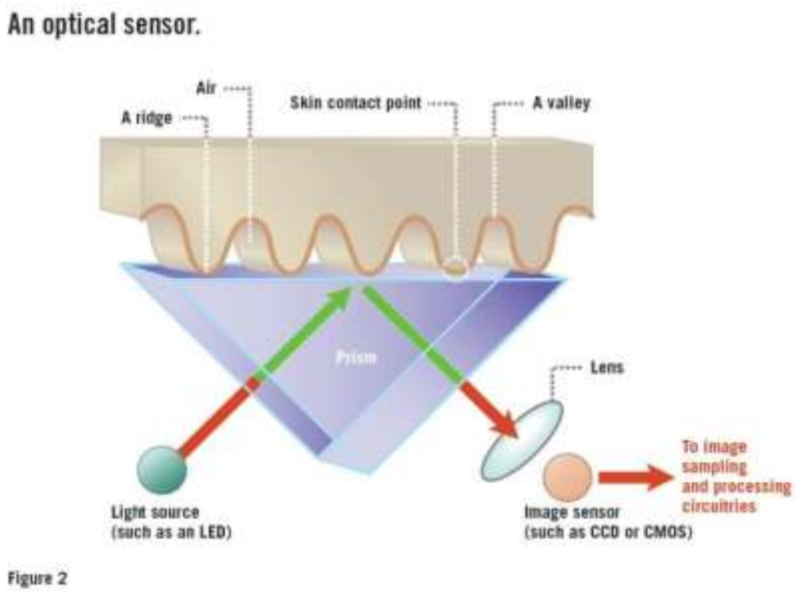

An optical sensor.
Air
A ridge
Skin contact point
A valley
Prism
Lens
To image sampling and processing circuitries
Light source (such as an LED)
Image sensor (such as CCD or CMOS)
Figure 2

Fig.6 Optical Fingerprint Scanner

.

The Capacitive scanner overcomes the drawbacks of optical scanners. The optical scanner can be fooled easily as it processes the image in 2D. Capacitive scanners are designed in a way more advanced manner. Instead of creating a image of a fingerprint, capacitive fingerprint scanners use arrays tiny capacitor circuits to collect data about a fingerprint. As capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to analyze and measure the details of a fingerprint. The charge stored in the capacitor will be changed slightly when a finger's ridge is placed over the conductive plates, while an air gap will leave the charge at the capacitor relatively unchanged. An op-amp integrator circuit is used to track these changes, which can then be recorded by an ADC.

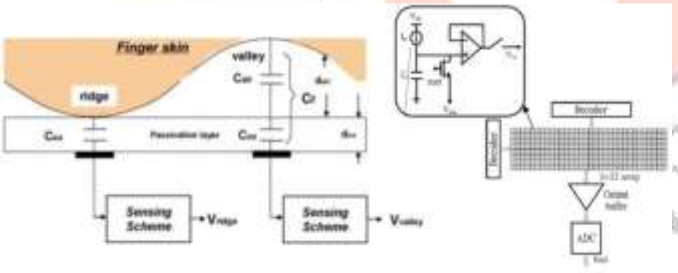


Fig.7 Capacitive Fingerprint Scanner

Due to the number larger number of components in the detection circuit, capacitive scanners can be a little expensive. Some early improvements attempted to cut the number of capacitors needed by using "swipe" scanners, which would collect data from a smaller number of capacitor components.

The latest feat in the fingerprint scanning is the ultrasonic scanner. To actually capture the details of a fingerprint, the hardware consists of both an ultrasonic transmitter and a receiver. An ultrasonic pulse is transmitted from the finger that is placed over the scanner. Some of this pulse is absorbed while some of it bounces back to the sensor, depending upon the ridges, pores and other details that are unique to each fingerprint.

The system uses UART interface for fingerprint technology. That means the Fingerprint sensor is attached with one UART IC that acts as its interfacing IC. Usually optical sensor fingerprint scanner is used with it. It provides secondary development, high-speed identification, high stability. It also has features like image processing, recording etc. The fingerprint scanner used here is GT511C3. Some of its features are:

1. High speed and high accuracy fingerprint identification technology
2. Ultra-thin optical sensor
3. Downloads fingerprint image from the device
4. Reads/writes fingerprints to/from the device
5. USB/UART communication protocol

2.5 Remote Voting

Till today, voting happens in the particular constituency and the voters have to vote in that constituency itself. There was no such provision that a voter from a different constituency shall vote from any part of the country, but online voting has made that possible. Now, while registering, the constituency shall be registered too, (which later can be changed in case of migration) and then the voter can cast his/her vote from any part of the country, saving time, effort and money.

2.6 Wi-Fi Interface

The connectivity between the voting booth and servers is to be maintained constantly. Not every EVM can be connected to the Internet using wires as it will cost a huge amount of wirings. Hence WI-FI modules have to be installed upon hi-speed and constant connectivity so that the voting don't stop or get interrupted. The servers have to be in constant connectivity so as to keep the authentication going on. Also the database has to be kept secured which shall be possible using secured programming, which is object oriented programming. Here the object is none but the data and has to be controlled by none another but admin.

2.7 Buzzer & EVM

The buzzer shall get activated once the voting is successful, or the voter has already voted or for any such errors. There shall be different tones to the buzzer allotted for such different occasions.

Whereas the EVM is connected to the UNO, this shall handle and control the operations upon it. Various candidates, who are contesting for the elections, have been allotted a separate button against their name upon the EVM. As the vote is casted the EVM shall notify it by light and by a beep. For only this system, for prototype purposes, a dummy model of EVM has been made. A miniature EVM of a basic kind.

2.8 Programming Details

The connectivity between the database (server) and the UNO has to be maintained which is the part of Wi-Fi, but to keep away the communication from any intrusion, and to securely verify, send and receive the data, is the programming part. The programming in this system is done OOP i.e. Object oriented programming, which was first introduced in C. Here the access specifier is termed as 'private' so that only the terms in the object an access them. It is similar as 'local variable', hence only the programmer i.e. admin can only access it. Every term is private so no one can either interfere in it or copy or open it.

2.9 Database Management

Database is referred to data of voters. "Central database" maintains details of all the voters residing in the country. Details comprises of particular voter's unique ID to identify, personal details, photographs and most importantly biometric details of the voter. These details are in general not revealed to any other organization and so these are maintained in additional servers with promising security. This data is used for matching of the voters' details at the time of verification process. Apart from this database, at each polling station and district or zone level, a "local database" is maintained which gives his or her unique ID and personal details only for reference. The servers handle this database and stored in them securely. Once a voter puts his/her fingers upon the scanner, and it is obtained, the images are then sent via the network to the database where they are scanned and the obtained result is then sent back to the UNO which shall the state whether its ok, not ok or already voted.

2.10 Flowchart

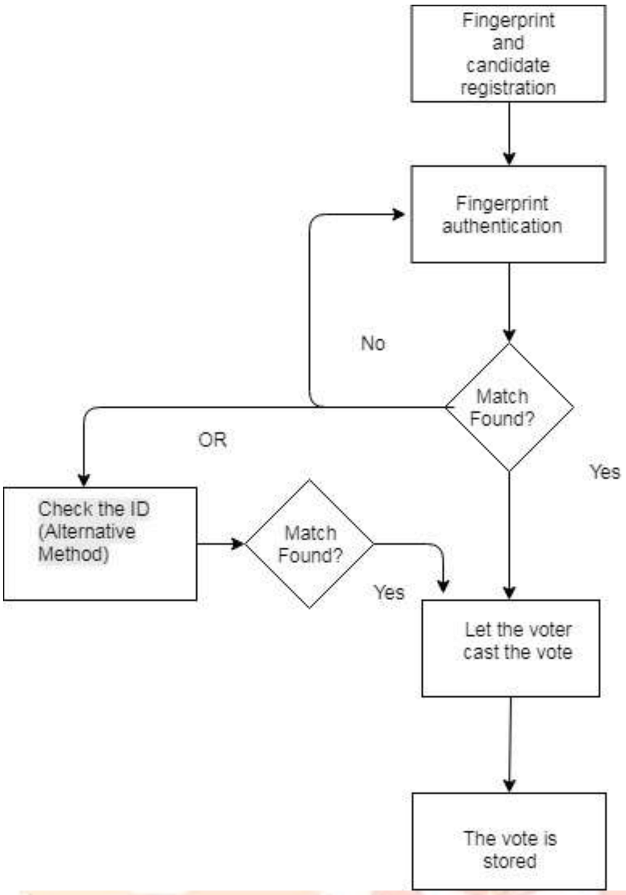

Fingerprint and candidate registration
Fingerprint authentication
No
Match Found?
OR
Yes
Check the ID (Alternative Method)
Match Found?
Yes
Let the voter cast the vote
The vote is stored

Fig. 8 Flowchart of IOT based Voting

2.11 Conclusion

The IOT based voting system has tried to overcome certain issues such as authentication of voters, remote voting etc. this shall truly encourage the voters as of now because the voting will be made possible from anywhere in the country. Also authentication means no rigged votings shall be possible and no such results. Although the system here has some issues. Fingerprints may not always be authentic in case of the elderly citizens (aged 90+), also if Iris scan is introduced, cataracts can cause errors. So a solid biometric identification technology is needed. But as a prototype, this seems quite promising to begin with human authentication.

2.12 Future Scope

- More such advancement is possible in the field of authentication. Face-recognition, Iris scan are one of them.
- Later on the voter can even get to know the exact percentage of votes, or if the constitution allows, his/her vote was given to which party, will be notified to them after the voting.

2.13 Result

Considering the problems of already existing systems, this system is developed in such a way to overcome them. With the implementation of this system in election process, surprising results can be obtained. The main motto of developing this system is to get a transparent voting procedure and improve the voting percentages in the country. It follows a simple procedure, consumes minimal man power, needs low power for operation, can save a lot of time, less prone to frauds and manipulations compared to already existing systems.

2.14 References

1 Patchava Vamsikrishna, Sonti Dinesh Kumar, Dinesh Bommisetty, “Raspberry Pi Voting System, A Reliable technology in voting system,” IEEE, 2016 International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT).

2 Talib Divan, Veena Gulhane, “A Fingerprint maching techniue using Minutiae based algorithm for voting system: A Survey” 978-1-4799-608S-9/1S/$31.00©201S IEEE.

3 Smita Khairnar, P. Naidu, "Secure Authentication for online voting system." IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICIIECS)2015.

[4] https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

IJCRT