IOT based Voting using Fingerprints: Review

Bais Anujsingh R[1], H.K Bhangale[2]
[1]M.E. Student, GHRIEM, Jalgaon.
[2]Prof, GHRIEM Jalgaon.
email-anuj.bais7@gmail.com

***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.**

***Keywords*— Arduino, EVM, Online voting.**

I. Introduction

Voting dates back to Before Christ (BC) period where the first democracy in the world, Greece used to have their leader to be elected by casing out votes against the eligible competitors.

Voting technologies have a surprisingly long history. In the United States, mechanical lever voting machines were first used for elections in 1892 and were commonly used in U.S. elections until the 1990s. In the 1960s, Electronic technologies began to appear with punch card counting machines. In the upcoming years, technologies such as DRE voting machines, ballot scanning machines and Internet voting began to appear. The U.S. was at the forefront of adopting many of these technologies. In the 1990s and the next 10 years of the new millennium, number of countries around the world also started to adopt these technologies.

The voting process is a huge ordeal for the election commission of the country since the EVMs used have been claimed to be rigged or hacked by a certain party. The votes casted are said to be 'diverted' to a certain party and caused a huge turn in the history of India. To improve its accuracy and efficiency so that good governance and proper candidate is elected to rule upon the nation and constituency, a smart voting method had to be implemented.

II. LITERATURE REVIEW

The system is to be designed so that it can:-

1. Improve the voting percentages
2. Reduce human interference.
3. Give rise to online voting and remote voting.
4. To make voting more efficient and secure.

PREVIOUS WORK

The voting methods are termed to be highly 'sensitive' and important and should be conducted in a very secure manner.

Earlier, there were many different techniques used to cast a vote.

There were ballots in which the name or stamp related to the candidate was inked on a paper and then submitted into a ballot box. The drawback was it required much time, paper and security. Then came the punched cards where the voters used to punch against the names. But the security issue still remained the same. The lever pulling too had an era in voting process. Here, the levers were assigned against each voter and pulling one of them would mean a vote has been casted to that candidate. But, mechanical failures, security reasons made this method obsolete too.

The voting method now in process is the EVM. Here the vote is casted by using an Electronic Machine in which the names of the candidates are present against a button. After pressing that button, a beep is heard, stating that the vote was casted to that candidate.

But the authenticity still remains an issue. In some places, random people come up and cast their votes, causing a 'rigged voting'[3].

FINGERPRINTS

The Biometrics of a Human body are its identity as they're unique for every human being on the planet. The biometrics namely are the Iris of the eyes, Fingerprints and toe prints, DNA etc. No other human being can posses the biometrics of someone else. Hence they become a medium of authentication or a proof that it belongs to a certain person only. That plays a great factor in the security and identification field. In this system, emphasis is given upon identifying the person by using its fingerprints. It is because they're easy to be recorded and take less time to process their authenticity. There are certain methods to capture the fingerprints [2]. There should be absolute certainty that the prints are recorded and verified correctly so that there should not be any false vote(s).

Starting from the voter registration [1], the voters have to be registered and their biometrics (eyes and prints) should be recorded. Then, at the voting process, they shall be verified not only by their ID, but also their biometrics as well.

The fingerprints can be recorded using either capacitive method or imaging (photo), using pressure, thermal sensing or dynamic capturing, where the AC voltage is recorded against the capacitance of the fingerprint.

Also there is Optical Fingerprint reader, in which image processing technique is used to analyze the fingerprint of the subject. This technique is widely used nowadays. UART is attached with the optical FPS to interface it with other devices.

A. Block diagram

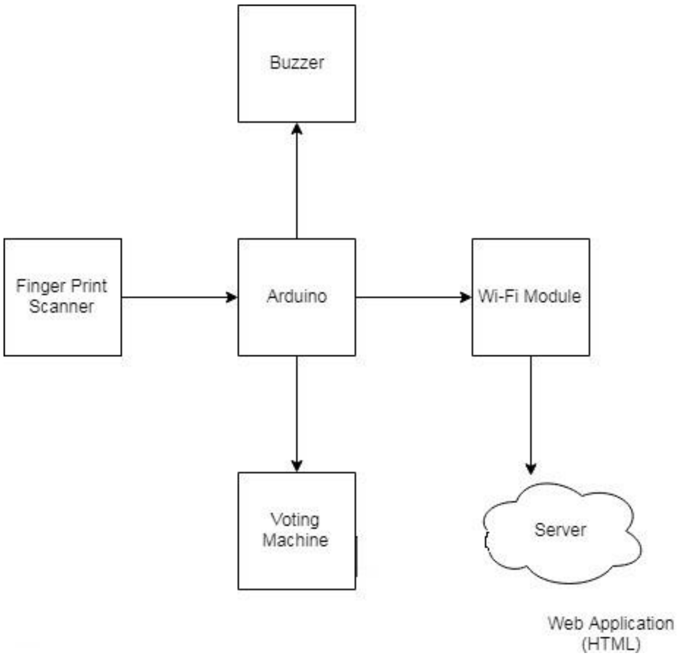

Fig.1 Block Diagram

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

A web application is to be made to make things happen in this system. The application shall keep the record of the candidates who have registered to vote, their biometrics, and the votes casted to which candidate etc.

B. Proposed system

The Arduino that operates the whole working of the system. The chip is the main operating unit in this system. It is connected to all the units in the system and operates with all of them. The FPS, Wi-Fi module, EVM, and also with the buzzer. It constantly has to monitor upon the operations of the devices altogether so that no error or false vote shall be enrolled or any eligible voter gets detained because the credentials didn’t match.

The FPS is used for authenticating the voter, by its credentials attached to the Aadhar card (Here the credentials shall be stored online upon a server which is very similar to that of an Aadhar card.

There shall be a central database where all the credentials shall be stored upon, which will be then verified at the time of voting. When a voter shall input its fingerprint, the database shall scan upon them and also will try to match them in its servers. Similar as a matching phenomenon.

Wi-Fi module and Servers make the happening of IOT.

III. ATMEGA328P

The Arduino family runs upon ATMega 328 technology. The Atmega328p is an 8 bit, 28 pin microcontroller belonging to the AVR family. It has 23 digital input/output pins and 6 analog inputs. 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.

Fig.2 Arduino UNO

A. ARDUINO UNO

Arduino UNO is microcontroller 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.

B. FINGERPRINT SCANNER

The function of FPS is to give authentication status to the microcontroller i.e. Arduino chip whether the voter is authentic (fingerprints matched), unauthentic (not matched) or has voted earlier. The output of FPS is given to Arduino and then it sends it to the server to check status upon the voter.

C. 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.

D. 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 microcontroller, which 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.

Expected Outcome

The outcome expected from the system proposed is an errorless or low error-rate technology which can revolutionize the voting method by having the tool of authentication in hand. Secured system, which will grant no interruptions or malfunctions in voting or in the identity of voters.

Conclusion

The proposed system sorts the issues of authentication, gives a fine new edge to remote voting, which can be the next big thing on the Internet. The basic purpose of this system is to have a transparent voting and improve the voting percentages in what is known as the largest democracy in the world.

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.

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/