



# **Biometric Secured Voting Machine to Avoid Bogus Voting Based on AADHAR CARD**

Umang Shah, Trupti Shah, Marteen Kansagara, Saagar Daxini

EC Engineer, Dept. of E.C., Gujarat Technological University, Government Engineering College, Modasa, Gujarat, India

EC Engineer, Dept. of E.C., Gujarat Technological University, Government Engineering College, Modasa, Gujarat, India

EC Engineer, Dept. of E.C., Gujarat Technological University, Government Engineering College, Modasa, Gujarat, India

EC Engineer, Dept. of E.C., Gujarat Technological University, Government Engineering College, Modasa, Gujarat, India

**ABSTRACT:** Today we all know that bogus(fake) voting is still major drawback in the elections. We can transform from ballot paper to electronics voting machine (EVM), but this problem cannot avoid completely. This paper attempt to solve this problem. Today we all have AADHAR CARD so the Government has all the data base of us including finger print and retina. As we all know that general election happened last year but no one really talks about the use of AADHAR CARD. So if we used that database effectively with the help of micro controller then we can completely overcome the problem of bogus voting. This paper shows how this problem can be solved with the help of combination of biometric finger print scanner and micro controller.

**KEYWORDS:** Micro controller, AADHAR CARD, Electronic voting machine (EVM)

## **I. INTRODUCTION**

This paper examines policy regarding the electronic approaches and developments towards avoidance of bogus voting and secured voting system. Finger print scanner is used for identity of voter and discussed other parameter which is implemented in this paper.

The user has to show his voter ID card whenever he goes to the polling booth to give vote. This is a time consuming process as the person has to check the voter ID card with the list he has, confirm it as an authorized card and then allow the person to poll his vote but this technique not give surety of right candidate voting. Thus, to avoid this kind of problems, we have designed a finger print based bogus avoidance of voting system where the person not required carries his ID and also avoid the bogus voting based on database of AADHAR CARD.

Today we all users have AADHAR CARD. First initially the database of finger prints which based on AADGAR CARD stored into the finger print scanner. When user put his/her fingerprint on figure print scanner, scanner checks it with previously stored in database. If finger print matched then EVM is enabling and the user is allowed to gives his/her vote.If that user comes again to give vote, a siren will blow that indicate the bogus voting.so we can easily prevent this kind of problems.For developing this kind of system we used AVR microcontroller.AVR is heart of entire system.

## **II. RELATED WORK**

In [1] author used to concept of design is suggest an election to choose the president of university, there are 4 candidate for this position, and there are 40 voter register in this election, the admin sponsors for register the voters, each voter can register after attending to the admin, give his name, id, and scan his fingerprint, then the admin submit this information to store in database, or the admin can get all voter's information with their fingerprints from official office. on the day of election the voters can participate by open the website of election from anywhere and cast their votes. when the voter want to vote, he will asked by the website to identified himself by his fingerprint, he will scan his finger (the same finger who submit before) and submit it to the system, then the system will return the decision for allowed or not allowed him to vote, voter is allowed to vote only for one time, the system can compute and display the results of

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

each candidate, also we add the pie chart in the results page to make the system more clear for user. the software is implemented completely as a .net managed code in #. In their project they use onlineafis.dll file which contains a single project onlineafis core sdk it basically handles the processing of fingerprint images and matching. In [2] author used biometric voting system using cryptography and stenography. the prototype builds based on secured and trusted framework for electronic voting. the system allows the voters to participate by using username and password. voter can enter the system and votes on the existing text during election date and the voter can see the result after the end of election date. E-voting is the process of using computerised systems in statutory elections, both to cast and count votes (e-counting). E-voting and e-counting open up elections to risks of fraud on a much greater scale than paper and pencil based systems. Current technology means that e-voting cannot deliver transparent, verifiable and anonymous elections.

## III. PROPOSED SYSTEM

### A. Working procedure of proposed system:

Biometric Secured Voting Machine to Avoid Bogus Voting Based on AADHAR CARD is basically an embedded system that makes the things easy avoidance of bogus voting during the time of elections. The user, who wants to poll his vote, has to punching the finger in finger print scanner at the counter at the polling booth. Based on finger print identify the identity of user. We know that user's finger print based on AADHAR CARD already saved in database of system.

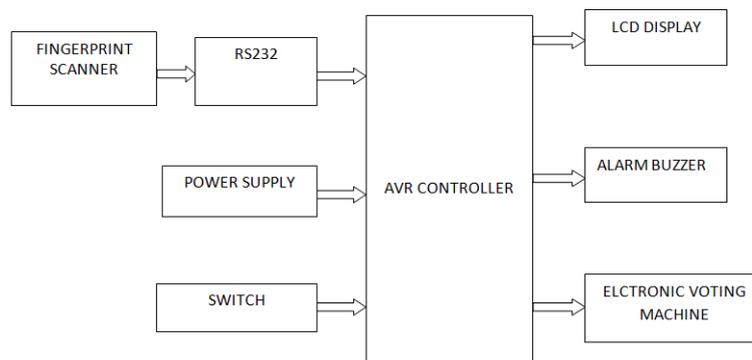


Fig. 1. Block diagram of proposed system

The working of system explained in two modes:

1. Enrolling mode
2. Punching and identification mode

When power on, whole system is active. Micro controller ready to gate signal from fingerprint sensor.

### Enrolling mode:

This mode is hidden part of system. By using Enrolling mode we store the few collection of finger print. In this mode we enroll the finger print of user by sending appropriate command. When user put the finger print on finger print scanner, generate the Image file of finger. Again put the finger print on finger print scanner for confirmation of valid finger print. Then generate another Image file. After completion of this step generate unique number of template file by combination of both Image file. This unique number store in the EEPROM of finger print scanner.

### Punching and identification mode:

After enrolling all finger print successfully, the system is ready for vote cast. Now user punches his/her finger on fingerprint scanner. During this mode the fingerprint of the user is compared with the finger prints already enrolled in the memory by algorithm which is embed in micro controller. If it is matched a message "IDENTIFICATION CONFIRM" will be displayed on LCD. If not then buzzer beeps three times which indicate the bogus user of voting. After confirmation of user, he/she permit to voting. Once the user presses the button corresponding to the candidate of

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

her/his choice, digital number is generated and sent to the control unit. Once the voting is over message “THANK YOU FOR VOTING “is displayed on LCD and buzzer beeps one time.”SORRY CANT ACCESS “message will be displayed if the same user tries to vote again. The system returns to the identifying mode and starts all over again for next voting.

## B. Description of the Proposed Algorithm:

- Step1: ON Power supply
- Step2: Active all devices
- Step3: Enroll the fingerprint of users which is given in AADHAR CARD
- Step4: user puts his/her fingerprint
- Step5: if finger print not matched go to step11
- Step6: if matched then allowed to voting
- Step7: Enter voting zone
- Step8: choose your candidate
- Step9: voting completed then buzzer beeps single time
- Step10: go to Step4
- Step11: buzzer beep three time which indication of unauthorized user
- Step12: go to Step4

## IV. RESULT ANALYSIS

The below figure 2 shows that how the system actually works. In this figure as you can see that the finger print scanner is attached with the AVR microcontroller and LCD. We used LCD for the display purpose. We used five templates for the experimental purpose.

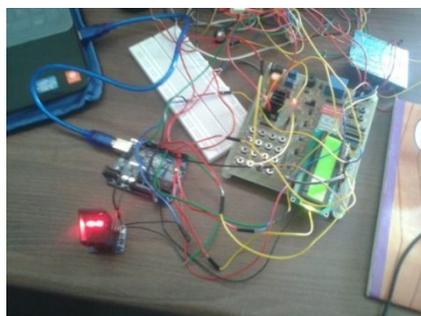


Fig. 2. Model of proposed system

The main two devices that we used in our project paper are:

- 1) AVR ATMEGA328:

The **Arduino atmega328** device contains a non-volatile 64KB Flash program memory that is both parallel programmable and serial In-system and In-application Programmable. The device is a single-chip 28-pins Microcontroller manufactured in advanced CMOS process.

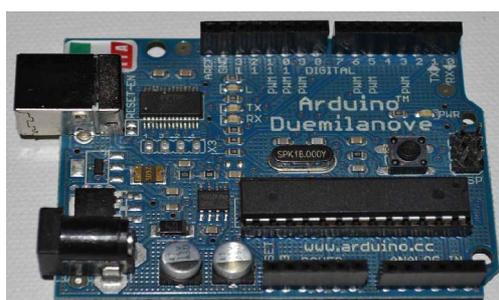


Fig. 3. microcontroller ATMEGA328

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

2) R305 optical sensor:

This is a fingerprint sensor module with TTL UART interface for direct connection to microcontroller UART or to PC through MAX232/USB-Serial Adapter. The user can store the fingerprint data in the module and can configure it in 1:1 or 1:N and mode for identifying the person. The FP module can directly interface with 3V3 or 5V microcontroller. A level controller (like MX232) is required for interfacing with PC serial port.



Fig. 4. R305 optical fingerprint scanner

The below figure 5 shows the final experimental result in which a person is giving his or her vote using a biometric system and that templates match with the previously stored templates and the person can vote. And second time that person trying to give vote with the wrong fingerprint that indicates fake voting and the system blows. So this way we can completely overcome the problem of bogus voting.

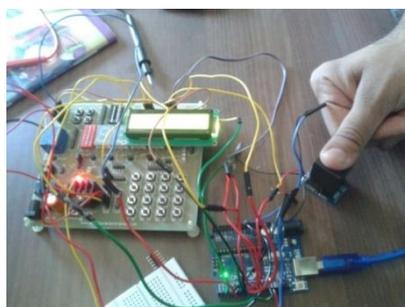


Fig. 5. Working of proposed system

## V. CONCLUSION

The basic idea of this project came from the ongoing election process, its campaign speeches delivered by party leaders against opposition alleging them of violating EVM during voting process by casting fake votes in favor of them. Thus to overcome such tactics and make voting process go paperless and fully secured- fingerprint based EVM is designed, on implementation of this machine, the election process of our country will be revolutionized. The project "biometric secure voting machine to avoid bogus voting based on AADHAR CARD" has been successfully designed and tested. This can bring a revolutionary change in the election procedures. As the normal EVM is the burning issue in recent days, this can be a solution for all the problems. Not only in India but also in other countries the face of the election procedure can be changed drastically using this technology.

## REFERENCES

1. Firas I. Hazzaa, Seifedine Kadry, Oussama Kassem Zein, 'Web-Based Voting System Using Fingerprint: Design and Implementation', International Journal of Computer Applications in Engineering Sciences, VOL II, ISSUE IV, DECEMBER 2012
2. Mayuri U. Chavan, Priyanka V. Chavan, Supriya S. Bankar, 'Online Voting System Powered by Biometric Security using Cryptography and Steganography', International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 7, December 2013