© 2017 IJSRST | Volume 3 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Biometric Secured Electronic Voting Machine with Embedded Security

S. Karthikeyan, J. Nithya
[1]Assistant Professor, Dept. of EEE, Annamalai University, Chidambaram, Tamilnadu, India
[2]PG Student, Dept. of EEE, Annamalai University, Chidambaram, Tamilnadu, India

ABSTRACT

Fingerprint verification is an important biometric technique for personal identification. The voting system is managed in a easier way as all the users should login by AADHAR card number and password and click on his/her favourable candidates to cast the vote. This features is a larger security in the sense that voter high security password is confirmed before the vote. The extra feature of the model is that the voter will ensure if his/her vote has gone to correct candidate/party. The votes are going to be done automatically, therefore saving an enormous time.
Keywords: Finger print, PIC Micro controller, AADHAR CARD.

I. INTRODUCTION

The term Biometrics is derived from the Greek word **Bios** means **"life"** and metrics means **"measures"** Biometric can be defined as the study of measuring those biological characteristics which include both physiological as well as behavioural characteristics that make human beings unique for recognition purposes. A Biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual. Various technologies explore, Biometrics have the potential for identification and verification of individuals for controlling access to secured areas or materials. Verification and Identification are two possible recognition processes which are performed each time when a potential user, attempts to access a system.

The user should show his voter ID card whenever he goes to the booth to poll his vote. This is often a time consuming method because the person needs to check the voter ID card with the list he has, make sure it is an authorized card and then enable the person to poll his vote. 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 is based on AADHAR CARD stored into PC.This Finger print reader reads the details from the tag.

This information is passed to the controlling unit for the verification. The controller reads data from the reader and compares this data with the already existing data.

If the data matches with the already stored information, the person is allowed to poll his vote. If not, a message is displayed on LCD and therefore the person isn't allowed to poll his vote. For developing this kind of system we used PIC microcontroller, PIC is heart of entire system.

II. METHODS AND MATERIAL

1. Conventional Voting Process:

This process is divided into four categories

Authentication : In this portion, every voter comes with his/her voter id in the center. The presiding officer verifies the id of the voter by matching it with the voter list comprising of the details of the voter. After authentication, the officer provides a ballot paper to the voter and marks his/her finger with a permanent marker.

Vote : After getting the ballot paper, the voter goes into covered booth which is placed in a corner of the room, marks the Symbol of the candidate of interest on the ballot, folds it and drops it in the ballot box.

Vote Counting : When the voting period ends, the presiding officer collects all the ballot boxes of the center and starts counting. While counting, it is very important to verify the proper votes. Only the presiding officer and Election commission nominated authorized members are eligible for this process.

Result : After finishing counting, the presiding officer announces the result and declares the winner of that particular center.

Conventional voting system requires a long period of time and lots of stationeries. It is also vulnerable against illegal vote casting. It is a manual system and there is always risk of manual errors during the counting.

Voter Confirmation: The voter should be confirmed clearly that his vote has been casted, and should be given a chance to modify his vote before it is finally casted.

No over-voting: The voters should be prevented from choosing more than one candidate option.

Under-voting: The voter may receive a warning for not voting, but the system must not prevent under voting.

Privacy: It should be confirmed that no one can access the information about the vote.

2. Electronic Voting System Requirements

Electronic voting system is not totally digital. It is combination of manual/traditional and automatic electronic voting system. Electronic Voting Requirements are given below:

Convenience: The system should allow the voters to cast their votes quickly in one session, and should not require many special skills or intimidate the voter.

Transparency: Both the Voters and candidates should be able to possess a general knowledge and understanding of the voting process.

Flexibility: The system should be flexible so that it can allow a variety of ballot question formats including open-ended questions

Accuracy: The system should record and count all the votes correctly.

Eligibility: Only authorized voters, who are registered, should be able to vote.

Uniqueness: No voter should be able to vote more than once.

3. Existing E-Voting System

Electronic voting system has brought revolutionary change in the traditional manual voting system. It can easily make that voting process simple and joyful. Main purpose of a Voting machine is to record vote and provide result very fast. The category "electronic voting" is potentially broad, referring to several distinct possible stages of electronic usage during the course of an election.

Electronic Voting : Electronic voting refers to any system where a voter casts his or her ballot using an electronic system, rather than a paper. Once recorded, an electronic vote is stored digitally and transferred from each electronic voting machine to a counting system.

Electronic Vote Counting*:* Electronic vote counting refers to the system that is used to tabulate ballots and award seats. It would be possible to vote using a non-electronic medium and then convert these votes to an electronic system and award seats through an electronic vote counting system.

4. Issues Of Existing Voting System:

There are many types of problems with EVM which is currently in use they are

- Accuracy: It is not possible for a vote to be altered e laminated the invalid vote cannot be counted from the finally tally.
- Democracy: It permits only eligible voters to vote and, it ensures that eligible voters vote only once.
- Security Problems :One can change the program installed in the EVM and tamper the results after the polling. By replacing a small part of the machine with a look-alike component that can be silently instructed to steal a percentage of the votes in favour of a chosen candidate. These instructions can be sent wirelessly from a mobile phone.
- Illegal Voting (Rigging) : The very commonly known problem Rigging which is faced in every electoral procedure. One candidate casts the votes of all the members or few amounts of members in the electoral list illegally. This results in the loss of votes for the other candidates participating and also increases the number votes to the candidate who performs this action. This can be done externally at the time of voting.
- Privacy: Neither authority nor anyone else can link any ballot to the voter
- Verifiability: Independently verification of that all votes have been counted correctly.
- Resistance: No electoral entity (any server participating in the e lection) or group of entities, running the election can work in a conspiracy to introduce votes or to prevent voters from voting.
- Availability: The system works properly as long as the poll stands and any voter can have access to it from the beginning to the end of the poll.
- Resume Ability: The system allows any voter to interrupt the voting process to resume it or restart it while the poll stands. The existing elections were done in traditional way, using ballot, ink and tallying the votes later. But the proposed system prevents the election from being accurate.

5. Different Steps of E-Voting

Button Verification*:* Button verification is very important. In every center, presiding officer will verify the button before voting starts. He will check every button by pressing them and sound coming from the pressed button will confirm its workability. The process is called “Pre armed check”. After verification of all the buttons the machine will start.

Finger Print Verification*:* Finger print or biometric voting process is a highly advanced system that allows enrolling and identifying millions of voters quickly and unmistakeably.

Use of biometric information will minimize the possibility of illegal vote casting. Ensuring quick and precise voter identification and enrolment is the cornerstone of any credible election. A full range of biometric parameters to identify the voters by fingerprints requires highly customizable software modules for both input and output settings. Fingerprint scanners are used here.

They provide a quick, easy, efficient, and secure measurement. For example the fingerprint of an employee is stored in a database that the scanner queries every time it is used. The scanner goes through two basic Boolean conditions when an individual’s print is scanned. First, the print is usually searched in a database of fingerprints. Once it is found, then it looks at the print to see what access privileges are associated with the print and compares them to the access they are trying to gain. If everything matches, then the subject is allowed access and if not, they are not allowed. A log of the event is usually stored for security purposes. The size of these devices is another reason for becoming so main stream recently. The objective of voting is to allow voters to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, Constitutional amendments, recalls and/or to choose their government and political representatives. Technology is being used more and more as a tool to assist voters to cast their votes. To allow the exercise of this, almost all voting systems around the world include the following steps:

- Voter identification and authentication
- Voting and recording of casted vote
- Vote counting
- Publication of election result

III. RESULTS AND DISCUSSION

Proposed Electronic Voting Machine

In the proposed machine there is no network connection, that’s why there is no chance to manipulate the result

remotely. There is no way to change the microprocessor code.

In this techniques the system consists of a tamper proof card where in all the records about the person are Stored in PC. The voter need not want to meet the officers at the polling booths instead of that they can go to the Machine directly. The pc will contain the complete information about the VOTER that is the details of the voter can get from the AADHAR card data base along with their finger print over the scanner. Then the machines will direct the voter to place his/her fingers on a finger print scanner for authentication.

After that the machine will perform a checking between two templates of the finger print. One taken from the live scan and the other stored previously in the system database. If these two templates are matched then the voter will get an OTP through the GSM modem. After receiving the OTP they want enter the same OTP into the keypad.

If the voter enters the wrong OTP the buzzer will on and therefore the person is not allowed to poll his/her vote. Finally the thank u message will be displayed on the screen after that the machine will ready for the next use. As the result of this process one person cannot cast the vote of another person.

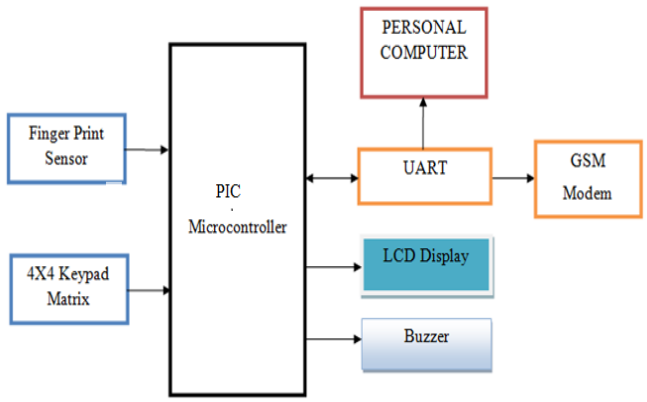


Figure 1. Block diagram of proposed system

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. We know that user's finger print based on AADHAR CARD already saved in database of system. 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 which is embedded in micro controller.

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

✓ **AVR ATMEGA328**

The Arduino atmega 328 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-pin Microcontroller manufactured in advanced CMOS process.

✓ **PIC Microcontroller**

The PIC Microcontroller is coded using the MP Lab software and later on it is dumped in the microcontroller using Flash Magic Software. This chip is the centre of heart that act as both the control and ballot unit of the voting machine. Since it also saves time of the voter who is casting their vote.

✓ **Finger Print**

The fingerprint identification module is used for verifying each and every person before allowing them to vote. This is the important module which is used for providing authentication to each and every user.

✓ **Unique Characteristics or Features of Fingerprints**

Each and every individual has a different or unique fingerprint. Even twins also share unique fingerprints. A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutiae points. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers can have these things to be identical.

✓ **Benefits and applications of Fingerprint Biometric Systems**

- Cheap
- Small size
- Low power
- Non-intrusive
- Easy to use

Fingerprint sensors are best for devices such as cell phones, USB flash drives, notebook computers and other applications where price, size, cost and low power are key requirements. Fingerprint biometric systems are also used for law enforcement, Forensics, dermatoglyphics, background searches to screen job applicants, healthcare and welfare.

IV. CONCLUSION

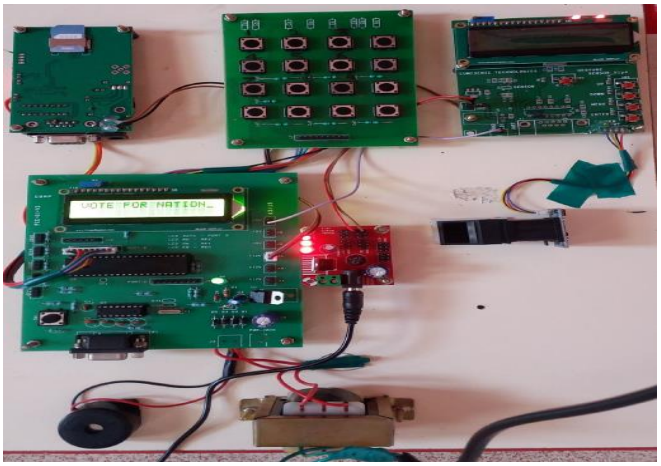
This paper "Biometric secured Electronic voting machine with embedded security" has been successfully designed and tested. As the normal EVM is the burning issue in recent days, this Electronic voting system will be a solution for all those problems in the following ways

- The voter's right is preserved.
- It is biometrically secured

The democracy of the nation is protected by using this safe and secured system.

V. RESULT ANALYSIS AND FUTURE SCOPE

In this project, a framework for electronic voting system based on fingerprint biometric is proposed and implemented with the Objective of eliminating bogus voting and vote repetition, less election expenditure, more transparency.



Electronic voting systems have many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, improved accessibility, greater accuracy, and lower risk of human and mechanical errors. It is very difficult to design ideal e-voting system which can allow security and privacy on the high level with no compromise. Future enhancements focused to design a system which can be easy to use and will provide security and privacy of votes on acceptable level by concentrating the authentication and processing section .In future face recognition can also include in the election process.

VI. REFERENCES

[1]. Ashok Kumar D., Ummal Sariba Begum T., "A Novel design of Electronic Voting System Using Fingerprint", International Journal of Innovative Technology & Creative Engineering (ISSN:2045-8711),Vol.1,No.1. pp: 12 19, January 2011.

[2]. Finger print liveness detection based on quality measures, IEEE, 08 July 2009

[3]. Prasad, H. K., Halderman, A. J., & Gonggrijp, R., "Security Analysis of India's Electronic Voting

Machines," International Journal For Research In Emerging Science And Technology, Volume-2, Issue-3.E-Issn: 2349-7610, March-2015.

[4]. Q. UIDAI.,"Role of Biometric Technology," AADHAR Authentication, (2012).

[5]. Yinyeh, M. O., & Gbolagade, K. A., "Overview of Biometric Electronic Voting System," International Journal of Advanced Research in Computer Science and Software Engineering, (2013).

[6]. Firas I, Haze, Seifedine Kadry, 'Biometrics-Based Voting System Using Fingerprint: Design and Implementation', International Journal of Computer Applications in Engineering Sciences, VOL II, ISSUE IV, DECEMBER 2012.

[7]. Mayuri U. Chavan, Priyanka V. Chavan, Supriya S. Bankar, 'Online Voting System Powered by Biometric Security using Cryptography International Journal of Advance Research in Computer Science and Management Studies, Volume 1, Issue 7, December 2013.

[8]. Khasawneh, M., Malkawi, M., & Al-Jarrah, O., "A Biometric-Secure e-Voting System for Election Process," Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), (2008), Amman, Jordan.

[9]. Prasad, H. K., Halderman, A. J., & Gonggrijp, R., "Security Analysis of India's Electronic Voting Machines," International Journal For Research In Emerging Science And Technology, Volume-2, Issue-3, E-Issn: 2349-7610, March-2015.

[10]. Q.UIDAI., "Role of Biometric Technology," AADHAR Authentication, (2012).