ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 2, February 2016**

# A Survey on E-Voting System Using Arduino Software

Rathna Prabha. S[1], Trini Xavier. X[2], Deepika. V[3], Iswarya. C[4]

Assistant Professor, Dept. of ICE, Saranathan College of Engineering, Trichy, Tamilnadu, India[1]

UG Student, Dept. of ICE, Saranathan College of Engineering, Trichy, Tamilnadu, India[2]

UG Student, Dept. of ICE, Saranathan College of Engineering, Trichy, Tamilnadu, India[3]

UG Student, Dept. of ICE, Saranathan College of Engineering, Trichy, Tamilnadu, India[4]

**ABSTRACT**: There are lots of methods to avoid fraudulence in voting systems, but we are not able to eradicate it completely. The objective of this project is to improve the security performance in the voting machine as well as to provide easy access to cast the vote by using finger print. Fingerprint is one of the unique identities of a human being which is being used in the aadhar system. By using arduino software and by using image processing we capture the finger print of every individual and the face of the individual is being captured. The polling of the vote is transmitted to PC through arduino communication. Face of the person captured is compared to aadhar details using LabVIEW. We also know about individual persons full details in the personal computer. In future, it could also be implemented using eye trace which will give more accurate results.

**KEYWORDS:** Arduino, Face Recognition, Finger Print, LabVIEW.

## I.INTRODUCTION

In paper-based elections voters cast their votes by simply depositing their ballots in sealed boxes distributed across the electoral circuits around a given country. When the election period ends, all these boxes are opened and votes are counted manually in presence of the certified officials. In this process there can be error in counting of votes or in some cases voters find ways to vote more than once. Sometimes votes are even manipulated to distort the results of an election in favour of certain candidates [1]. In order to avoid these shortcomings the government of India came up with Direct-recording electronic (DRE) voting system which are usually referred as Electronic Voting Machines or EVMs. These devices have been praised for their simple design, ease of use and reliability. However it has been found that EVMs are not tamper proof and are easily hackable. Moreover this attacks, hardware as well as software, go without any detection but are quite simple to implement. This made us to bring forth a system that is secure, transparent, reliable as well as easy to use for the citizens. Biometric e-voting systems are not a phenomenon anymore they are being actively used in countries like Ghana and Ireland and are spreading to many other developing nations. In this project we propose an idea to avoid fraudulence in mechanism to make e-voting in India a reality. It improves the security performance and avoid forgery vote because naturally one human finger print is different from other human.
From the paper titled "A Biometric-Secure e-Voting System for Election Process" the authenticated voters and polling data security aspects for e-voting system was discussed. They insured that vote casting cannot be altered by unauthorized person. The voter authentication in online e-voting process can be done by formal registration through administrators and by entering one time password. In offline e-voting process authentication can be using Iris reorganization which enables the electronic ballot reset for allowing voters to cast their votes. In the paper titled "Security Analysis of India's Electronic Voting Machines" they present a security analysis of a real Indian EVM obtained from an anonymous source. They also described the machine's design and operation in detail, and they evaluated its security, in light of relevant election procedures. They concluded that in spite of the machine's simplicity and minimal software trusted computing base, it is vulnerable to serious attacks that can alter election results and violate the secrecy of the ballot. In the paper titled "Overview of Biometric Electronic Voting System" the overview of the development and implementation of Biometric Electronic Voting System Software has been discussed. This is integrated with a biometric fingerprint machine to scan the finger print of eligible voters during the registration process

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 2, February 2016**

and for the authentication or verification on Election Day. They implemented on personal computers over a Local Area Network at each polling station.

This paper is structured as follows:
Section 2, shows the Block Diagram of the E-Voting system. Section 3, we have discussed in detail about the hardware configuration of the Arduino board UNO. In section 4, we discussed about the working of the finger print sensor. The conclusions arrived, based on the results in section 4.

## II.BLOCK DIAGRAM

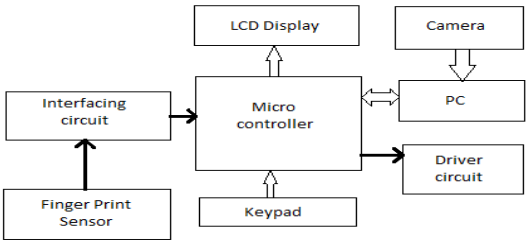


**Fig. 1. Block diagram of E-Voting System.**

The above block diagram projects the microcontroller based architecture of the E-Voting system. Thus, the data is stored and the information is transferred to the personal computer. Finger print sensor is interfaced with the microcontroller through the processor circuit. The related data is stored in the microcontroller. The microcontroller transfers the related information on the LCD display and PC.

## III.HARDWARE CONFIGURATION

There are many different types of electronics hardware development boards featuring embedded processors and the most famous species like Raspberry pi, Beagle Bone, Arduino Galileo. The embedded world evolved very differently there were too many choices for processors, which were mainly chosen for price and features. The devices like Raspberry pi and Beagle Board are best for handling media such as video. They are designed to function on a much higher level with already integrated hardware that takes care of things like Ethernet, video processing, large quantities of RAM and an almost unlimited amount of storage space. In the other side the Arduino is an excellent choice if we have a project requiring sensors (and decent memory and processing power), monitoring, or have productivity-related applications (Galileo has a real time clock.) Galileo could be used to develop smart everyday "things" with lots of sensors, such as health monitoring, security system, home automation, fitness devices, or simply be an inexpensive personal computer running Linux sans all things by Arduino.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 2, February 2016**


**Fig. 2. Arduino board UNO**

The Fig. 2 shows the hardware figure of the arduino board UNO. The above shown arduino board is of the type of ATmega328 arduino board .

| **Microcontroller** | **ATmega328** |
|---|---|
| Operating Voltage | 5volts |
| Input Voltage(limits) | 6-20V |
| Digital I/O pins | 14 |
| Analog input pins | 6 |
| DC current per I/O pin | 40mA |
| Flash Memory | 32kB(ATmega328) |
| SRAM | 2kB(ATmega328) |
| EEPROM | 1kB(ATmega328) |
| Clock | 16MHZ |

**Table. 1. Specifications of Arduino Board UNO**

The above Table. 1 shows the hardware specifications of the arduino board ATmega328 UNO. It shows the range of the operating voltage, digital input and output pins and the memory range.

*A. Finger Print Stage:*
This system registered the users that consider as authority to access control in the enrollment model. Each user in this stage will take the Aadhaar ID number that is saved in the database. In fingerprint stage we used two important functions feature extraction and the matching function which has been discussed below.

*B. Feature Extraction:*
The feature extraction is responsible for expressing fingerprint's unique characteristics adequately such as directions of the lines, terminals of lines, bifurcation and so on. To ensure the accuracy of comparison, the method of feature extraction must extract useful features as such as possible; meanwhile, filter false features for various reasons. There are two kinds of features in fingerprint images: global feature and local feature. Global feature can reflect overall shaper of fingerprint, which usually applies to fingerprints' classification, the process of extract global feature frequently belongs to procedure of fingerprint classification. The Local feature can reflect minutiae of fingerprint, usually applies to fingerprints' comparison. Strict feature extraction means local features' extraction. Two fingerprints often have the same global features, but their local features cannot be exactly the same. The important information of fingerprints' local feature is following: terminals, bifurcations, branch points, isolated points, enclosures, short lines and so on. In fact, not all the fingerprints have these two features, it often be used as fingerprints' sub-matches. This system uses terminals and bifurcations in feature extraction and matching algorithm.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 2, February 2016**

*C. Feature Matching:*

The matching function, features extracted from the input fingerprint is compared against those in a database, which represents a single user (retrieved from the system database based on the claimed identity). The result of such a procedure is either a degree of similarity (also called matching score) or an acceptance/rejection decision. There are fingerprint matching techniques that directly compare gray scale images using correlation-based methods, so that the fingerprint template coincides with the gray scale image. However, most of the fingerprint matching algorithms use features that are extracted from the gray scale image. A large number of approaches to fingerprint matching can be found in previous work. In this proposed work we used the matching algorithm that support the optical fingerprint reader module SFG algorithm is specially designed according to the image generation theory of the optical fingerprint collection device. It has excellent correction &tolerance to deformed and poor-quality fingerprint and work with both 1:1 and 1:N.

*D. Face Recognition:*

Every human could be identified by the faces and could be easily recognised by the faces. Early face recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes. Thus the face recognised could be both verified and identified. Thus, by using face recognition here we could avoid the fraudulence.

*E. LabVIEW:*

In this paper we are using LabVIEW. LabVIEW [Laboratory Virtual Instrument Engineering Workbench] is the graphical programming language. Designing of LabVIEW is used with hardware supported by National Instrument MYRIO driver. USB communication cable, PCI device with analog input also include in that. There is a lot of built in analysis function available in LabVIEW, which is used to easily create the program for complementary problem. Filter, PID control algorithm, converter and correction factor, simulated signals these are commonly used library.

## IV.WORKING

The finger print sensor is interfaced with the microcontroller. The processor activates the finger print sensor at the time of finger is placed in the sensor. Then the related data is stored in the microcontroller. The microcontroller transfers the related information to PC. When the human places the finger on the finger print sensor, the sensor sends the corresponding data to the microcontroller. Microcontroller receives the data from the finger print sensor. Then compared with the stored data if the person finger is valid for that voter name mentioned in the voter ID card it is displayed in the LCD display and the person is eligible for voting. If the authentication is failed then the particular person is not eligible for voting.

## V. CONCLUSION

Thus, the arduino controller could be interfaced in LabVIEW environment. The real time vote monitoring is made possible and finding of repeated voting by same voter could be detected easily.

## REFERENCES

[1] 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.
[2] 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.
[3] Q. UIDAI., "Role of Biometric Technology," Aadhaar Authentication, (2012).
[4] Yinyeh, M. O., & Gbolagade, K. A., "Overview of Biometric Electronic Voting System," International Journal of Advanced Research in Computer Science and Software Engineering, (2013).
[5] McGaley., Margaret., "Irish Citizens for Trustworthy Voting," 6 July 2004.
[6] UIDAI, "Biometrics Design Standards For UID Applications," 2009.