Two-Way Authentication Secured Voting System Using Biometric Fingerprint

PraneshwarP, RahulR, Aravind A R

Department of Electronics & Communication Engineering,

Prince Shri Venkateshwara Padmavathy Engineering College,Chennai 127

Abstract

Indiabeing the largest democracy faces a lot of issues during elections. Lot of controversies are reported about voting system, voting machines, authentication of voting, corruptions during elections etc. This paper describes a secured system that can eliminate such controversies involved during the elections in our country. A prototype has been made and tested successfully with an Arduino Mega 2560microcontroller-based RFID facilitated electronic voting machine possessing aTwo-way authenticated fingerprint security. This device was developed by interfacing fingerprint sensor, a keypad, GSM module, RFID reader, an LCD and a personal computerto an Arduino Mega. Algorithm was developed and coded using the Arduino IDE. The main purpose of this system is to give a straight and fair elections and to curb all other factors that affect it, this goal has been achieved by providing dual verification of the voters based on their fingerprint and unique id. In this system all the relevant information is taken from the voters and are stored in the microcontroller, then they are provided with unique ID. The process of verification involves matching of this id and fingerprint from the microcontroller. After verification process, the voter receives a message to his/her mobile number via GSM technology. To avoid delay in the announcement of results, there is a solution where when the polling officer verifies his authenticity, he/she can get the vote count by pressing the designated number on the keypad. So, this is a faster and more secured way of holding elections. This system is secured, reliable and also cost- effective.

Keywords: **E-voting, Election, Finger-print, RFID, Arduino.**

1. INTRODUCTION

Elections make a fundamental contribution to democratic government. Elections enable voters to select leaders and to hold them accountable for their performance in office. So, the process of the voting should be free from discrepancies. There were many voting systems earlier in the world such as, ballots, electronic voting machine, punch card and direct electronic voting machines (DRE), but each of these systems has several drawbacks. Many of these systems involve manual counting of votes, so there are more chances of error, such as false counting influenced by the involved parties and it takes much time to announce results. As technology evolves over time, the need for a better, faster, more convenient and secure e-voting is an essential requirement. As the right to vote is an essential right of every citizen, it should not be compromised by various fraudulent activities. Biometric verification such as fingerprint verification, iris verification is the best way to get rid of this menace. As fingerprint is unique for everyone, there couldn't be any fraudulent activities. Generally, the announcement of results takes about months and as a result of technology advancement the results can be announced earlier than other conventional systems.

2. RELATED WORKS

A number of related works exist in literature. Review of recent works, merit and demerit are thus presented.In general, our research covers the literature review from various sources based on secured biometric voting system.

This device was developed by interfacing fingerprint sensor, a keypad, GSM module, real time clock, an LCD and a personal computer to an Arduino Mega. Algorithm was developed and coded using the Arduino IDE. The unit stores voter data, which includes biometric information, during registration and randomly assign voting pins to registered voters to their given mobile numbers. Prior to voting, it checks for a match with the stored data during the authentication by comparing biometric and then pin of a voter to that in the database. Upon successful authentication, the voter is allowed to cast their vote, either in open ballot or closed ballot mode. The device collates result of voting including time of each vote and can deduce the winner based on majority votes [1].

This project is used to provide easy and more secured election process using biometric and face recognition. More commonly the biometric is secure than any password or ID. But in recent times, there is many chances to create fake finger prints as like originalone.To overcome this problem, face recognition sensor can be used next to the step of fingerprint identification. The voter's face detected and stored in the database to recognize the person. If the match occurs,then the person is allowed to cast their votes only once. This provides security against duplicate vote and fraudulent action [2].

The proposed system is Implemented using RFID and IoT (Internet of Things) to improvise the security mechanisms.Here, an active RFID tag is used in place of voter id where the system can scan the tag and matches with the fingerprints collected in the Aadhar database [3].Introducing a two-step verification which will help avoid the middle man attack i.e., only when the voter is physically present the fingerprint of the voter can be registered and only then the OTP will be sent to user's mobile number this in turn prevents fake voters [4].This paper describes the design, operation of smart EVM using microcontroller, RFID, GSM technology to improve the election process by avoiding the electoral fraud and to ensure safety, security, reliability, guarantee and transparency and smooth conduct of elections in the country [5].

Another proposed system is made and tested successfully with an Arduino UNO based Aadhar facilitated electronic voting machine. The process of verification involves matching of id and fingerprint from the database [6]. The system consists of tamper proof card which is used to store all database. And the voter can directly to go the machine to vote, there is no need of polling officer [7].

In this modern age of digitization, Bangladesh Election Commission (EC) still uses manual system during election for vote casting. Recently, it is considering to introduce Electronic Voting Machine (EVM) in parliamentary elections though EVM is not entirely automated and has many limitations. In this work, we have designed an automated biometric voting system with a convenient user interface and integrated database system containing all voters' information. Casted votes will be counted automatically at the end of the voting process and result will be generated centrally with less time [8].

The basic idea of this project is to create an electronic voting machine with the inclusion of biometric fingerprint sensor, each voter is entered into the system only after being recognized and checked with the given database of enlisted voters. Once the corresponding fingerprint is matched, the voter will be allowed to proceed for choosing their preferred candidate from the panel of buttons. The final vote is then displayed onto an LCD for the satisfaction of voters [9].

3.Methodology

The proposed system block diagram is shown in Figure 1 and consists of an Arduino Mega 2560 as the main unit of the system. The sub-units interfaced to the Arduino include the keypad, fingerprint sensor, RFID reader, liquid crystal display (LCD) and a GSM module. The software aspect was programmed using the Arduino sketch on a personal computer and uploaded to the Arduino board Via USB port. External power supply was thereafter used to power the system.
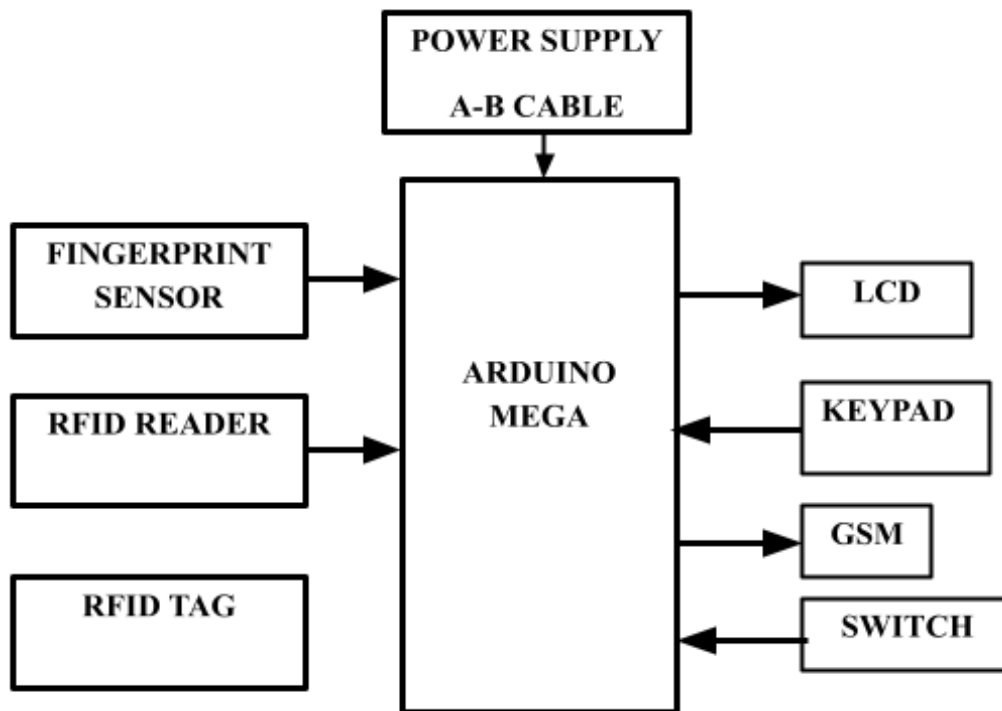
Figure 1 Block diagram of the proposed system

Initially, there will be a 'n' number of RFID tags. Each RFID tag has its own unique id number. The Polling Officer will have one RFID tag. Then he verifies his fingerprint and starts the polling. And the public voters cast their vote after their verification process. Each ID number is assigned to each fingerprint. So, there is no way of cheating. After Polling Officer places his fingerprint, there will be three options displayed on the LCD display. They are: 1. TOT (Total vote count), 2. PL-START (Start Polling), 3.PL-STOP (Stop Polling). After voting successfully, an acknowledgement message will be sent to the corresponding voter's mobile number.

In our proposed voting process, verification for authorized voter is done with the help of fingerprint scanner, which ensures that voter is registered voter and only authorized voters are allowed to cast votes. This also assures the physical presence of the voter. Multiple votes of single voter cannot be casted as only one vote per user is allowed. If the voter tries to cast multiple votes alarm will be activated and the respective personals will be informed through SMS via GSM. Thus, our system eliminates the chances of multiple voting, fake votes, booth capturing which makes our system more secured.This system will abort malpractices carried out under the name of elections and will ensure unique allocation of votes. As the Polling Officer has the authority to start and stop the polling, there is no chance of malpractices. In case of finger mismatch or multiple voting, a message will be sent to the Polling Officer's mobile number through GSM.

4. RESULTSANDDISCUSSION

The results highlight how the components, methods and interconnections described in methodology are geared towards solving the issues of voter fraud, voter impersonation and result rigging as stated earlier.

4.1 Experimental setup

In this section, we estimate performances of the proposed system method, with Arduino Mega 2560 as its microcontroller, the instructions provided to the Arduino is executed and the desired results are obtained. Figure 2 depicts the experimental setup of the Two-Way Authentication Secured Voting System.
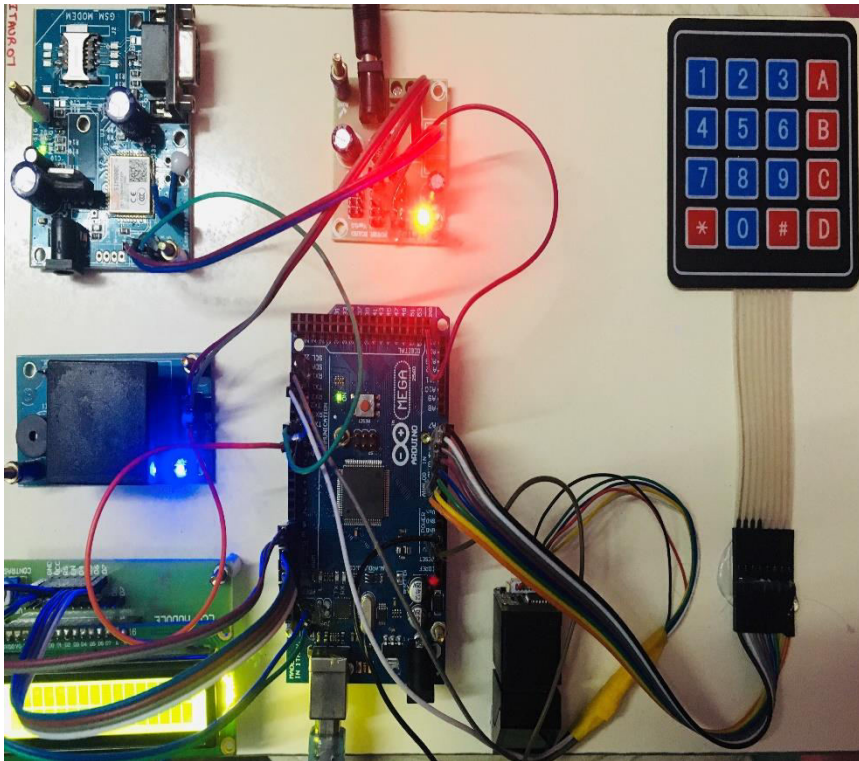
Figure 2 Experimental Setup of Proposed System

The below mentioned results are the output that is obtained during the execution of the proposed system.

4.2 Initial voting phase

Initially the Polling Officer places his/her RFID tag and then places his fingerprint on the fingerprint scanner to initiate the election process in the corresponding booth. The message "PLACE VOTER ID" is being displayed in the LCD monitor as shown infigure 3.

Figure 3 Initial Voting Phase

When the Polling Officer places his/her RFID tag on the RFID reader, the RFID reader scans the tag and displays "WELCOME PO PERSON:". Then the Polling Officer places his fingerprint on the fingerprint sensor. If the fingerprint is authentic and is matched, then the LCD displays "FOUND:". Figure 4 depicts the verification process of RFID.

Figure 4 Verification of RFID Tag

Figure 5 depicts the fingerprint verification process after placing the fingerprint. The fingerprint sensor switches on once the welcome message is displayed.

Figure 5 Fingerprint Verification Process

4.3 Polling Starting Phase

After the verification of Polling Officer's fingerprint, three options will be displayed on the LCD display. They are: 1.TOT (Total Vote Count), 2. PL-START (Start the polling) and 3. PL-STP (Stop the polling). Figure6depicts this phase.

Figure 6 Polling Officer's Options

When the Polling Officer presses 2 to start the polling, the polling is started and the public voters can cast their vote after verification. Figure7 depicts the polling starting phase.

Figure 7 Polling Starting Phase

4.4 Candidate Information Zone

The voters can cast their vote by pressing the corresponding number of the candidate. Figure8 depicts the candidate information zone.

Figure 8 Candidate Information Zone

After pressing the corresponding number, the vote is casted and it displays the message "VOTED SUCCESSFUL".

4.5 Total Count and Authentication Phase

When the Polling Officer presses 1, the total vote count is displayed on the LCD display. Then the authentication problems such as fingerprint mismatch and voting multiple times are found and displayed on the LCD screen and a message will be sent to the Polling Officer's number. Figure 9 depicts the total count of votes.

Figure 9 Total Count and Authentication Phase

Figure 10 depicts the fingerprint mismatch message.


Figure 10 Fingerprint Mismatch Message

Figure 11 depicts the already voted message.

Figure 11 Already Voted Phase

4.6 Acknowledgement Message via GSM

After casting votes, each voter receives an acknowledgement message to their mobile phones which is shown in figure 12 and the Polling Officer receives any message regarding violations performed during voting to his/her mobile phones with the help of GSM technology.
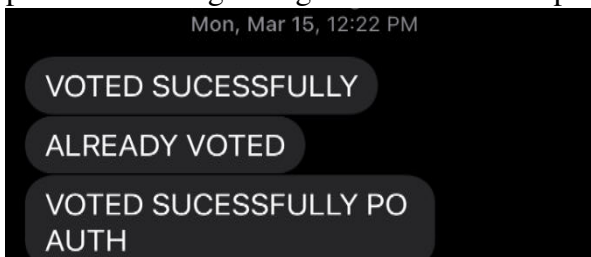
Figure 12 Acknowledgement message via GSM

5. CONCLUSION

Electoral process in many developing nations is characterized with fraud and failure and this in most cases leads to crises. Through this project, the proposed system puts forward an ideal electronic voting machine that uses a microcontroller to handle all the processes. This system is easy to use, convenient and economic in comparison with the conventional paper- based vote casting scheme and current e-voting system. The main advantage of using this system is that as fingerprints of everybody is specific and unique, the duplication of votes can be avoided. In total, this system overcomes most of the problems faced during the voting period by the paper ballot system. The efficiency of this system depends upon the authentication using fingerprint sensor and its usability. This will surely ensure a safer voting method which is very much what is required for a healthy growth of a developing nation. In this paper, the proposed Fingerprint based voting system is better and faster than previous systems. The new system prevents access to illegal voters, provides ease of use, transparency and maintains integrity of the voting process. The system also prevents multiple votes by the same person and checks eligibility of the voter. Additionally, the voter will receive an acknowledgement message to their mobile phone via GSM technology enabled in the proposed system. Fingerprint based voting system has provided chance to avoid invalid votes. It reduces the polling time, reduces the staff present in the voting center, it provides easy and accurate counting without any troubles, provisioning of voting preventive measures.The pursuits of knowledge to create an acceptable electronic voting system envisage the importance of the authentication method.

6. REFERENCES

[1] Abdulkadir H, Alkali Emmanuel G, Dada Dauda E, Sadiq Mshelia and Onundi O (2019) 'Design and Development of an Arduino Based Electronic Voting System', International Refereed Journal of Engineering and Science 8 48-57.

[2]Ganapathi T, Sathishkumar D (2019) 'SAFE AND SECURE SMART ELECTRONIC VOTING MACHINE USING BIOMETRIC', International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056 p-ISSN: 2395-0072 Volume: 06 Issue: 03.

[3] Mansingh, PM Benson, T. Joby Titus, and VS Sanjana Devi (2020) 'A Secured Biometric Voting System Using RFID Linked with the Aadhar Database', In 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1116- 1119. IEEE.

[4] Narayanan N, Ch. Surya Pradeep, Piyush Gulati, G. Raj Bharath, S.Nivash (2019) 'Design of Highly Secured Biometric Voting System', International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-5S3.

[5] Surendra Rao B, Prasanth E, Siva Sai Teja R and Sandeep Y (2019) 'RFID based Smart Voting System', International Research Journal of Engineering and Technology 61577-1580.

[6] Santosh Kumar Shaw, Sashank Poddar, Vivek Singh, Sudip Dogra (2018), 'Design and Implementation of Arduino Based Voting Machine' IEEE.

[7] Peter, Ms Mary Varsha, Ms V. Priya, Ms H. Petchammal, and Dr N. Muthukumaran (2018) 'Finger Print Based Smart Voting System', Asian Journal of Applied Science and Technology 2, no. 2: 357-361.

[8] Mahboob Karim, Nabila Shahnaz Khan, AshratuzZavin, Shusmoy Kundu, Asibul Islam, Brazab Nayak (2017) 'A proposed framework for biometric electronic voting system', IEEE International conference.