iJET EXPLORE International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 5 No. 6, June, 2015

Finger Print Enabled Electronic Voting Machine with Enhanced Security

[1]Syed Razwanul Haque, [2]Miah Md. Asaduzzaman, [3]Prasanta Bhattacharjee, [4]Akhlak Uzzaman Ashik, [2]Robi Kormokar

[1]Lecturer, Dept. of Electrical and Electronic Engineering,Metropolitan University, Sylhet, Bangladesh
[2]Assistant Professor, Dept. of Electrical and Electronic Engineering, Metropolitan University, Sylhet, Bangladesh
[3]Dept. of Computer Science and Engineering, MetropolitanUniversity, Sylhet, Bangladesh
[4]Dept. of Physics, Shahjalal University of Science and Technology, Sylhet, Bangladesh

ABSTRACT

Electronic voting machines are getting popular day by day to conduct Election in densely populated countries. Bangladesh has almost 90 million voters and their biometric information. To make proper use of this information in Election for faster and transparent voting process, a Finger-print enabled EVM has become a necessity. Currently available Biometric integrated EVMs have some issue with their security, vulnerability and power backup. This paper is about the design and construction of a Finger-Print enabled electronic voting machine (EVM) with greater security and power backup compared to the existing EVMs of this type. The machine is integrated with finger print and various steps of hardware security layers. The proposed design ensures accuracy, transparency, security and faster result processing in Election.

Keywords: *EVM, Security, Finger print, Biometric.*

1. INTRODUCTION

A. 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. All the above mentioned problems make Electronic Voting Machine the necessity of a modern democratic world.

B. 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.

• Auditability: It should be possible to verify that all votes have been correctly accounted in the final election tally, and there should be a reliable and demonstrable authentic record, in terms of physical and permanent audit.

• 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. DIFFERENT STEPS OF E-VOTING

A. 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.

B. Finger Print Verification*:* Finger print or biometric voting process is a highly advanced system that allows enrolling and identifying millions of voters quickly and unmistakably. Use of biometric information will minimize the possibility of illegal vote casting. Ensuring quick and precise voter identification and enrollment 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 mainstream 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 [2].

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

Voter identification is required during two phases of the electoral process: first for voter registration in order to establish the right to vote and afterwards, at voting time and to allow a citizen to exercise their right to vote by verifying if the person satisfies all the requirements needed to vote (authentication) [3]. The field of biometrics was formed and has since expanded on to many types of physical identification. Still, the human fingerprint remains a very common identifier and the biometric method of choice among law enforcement [1]. These concepts of human identification have lead to the development of fingerprint scanners that serve to quickly identify individuals and assign access privileges. Finger print recognition, the electronic methods of recording and recognizing an individual finger print, advanced substantially during the last decade of the 21th century [4].

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.

A. 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.

B. 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.

Electronic Voting Machine is a simple electronic device used to record votes in place of ballot papers and boxes which were used earlier in conventional voting system [4]. It is a simple machine that can be operated easily by both the polling personnel and the voters. Being a standalone machine without any network connectivity, nobody can interfere with its programming and manipulate the result. Keeping the erratic power supply position in many places in the country, the machines have been made to run on batteries. It has mainly two units: Control unit and Ballot unit. The Control Unit is the main unit which stores all data and controls the functioning of EVM. The program which controls the functioning of the control unit is burnt into a microchip on a "one time programmable basis". Once burnt it cannot be read, copied out or altered. The EVMs use dynamic coding to enhance security of data transmitted from ballot unit to control unit. The new EVMs have also got real time clock and date-time stamping facility which enables them to record the exact time and date whenever a key is pressed. After the voting is completed and the close button is pressed, the machine does not accept any data or record any vote. Through the press of "total" button, the control unit can display the number of votes recorded till that time which can be cross checked with the register of voters. The display system of the control unit shows the total number of votes polled in a polling station and the candidate-wise votes polled in the machine when the 'result' button is pressed by the counting staff in the presence of counting agents at the counting center. The control unit can also detect any physical tampering made with the connecting cable and indicate the same in the display unit [6].

4. 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. All the results are saved in a powerful SD card. It has real time clock and date. Battery unit is connected with control unit and ballot unit.

A. Hardware Units:

The machine has two units which are totally separated. They are given below:

• *Control Unit:* This unit maintains the whole system. It has a reset button, clear button, stop button, cancel button, result button. When reset button is pressed, then the machine is ready for vote. A sound confirms presiding officer that the machine is ready for voting.

If presiding officer presses the reset button twice, then it generates a warning signal and presiding officer can use the 'Cancel button' to cancel the previous reset condition. After successful cancellation, the unit generates another sound. When the voting period is finished, presiding officer can end the voting session by pressing ''Stop' button. There is a display on control unit for displaying result. After ending the session, the presiding officer has to press the 'Result' button for getting the total count of each candidate. Individual counts of the candidates are displayed on the display of the unit. When results are shown on the display, a light is turned on with a message that the Voting session of the center has been completed.

• **Ballot Unit:** The ballot unit is comprised of candidates' names, their voting signs and a button beside each of them. When the verification procedure is done, the voter goes into the ballot unit room. Then the presiding officer presses the Reset button and makes the machine prepared for voting and the voter casts his vote. After the successful casting of a vote the machine will bell a sound and voice message will be heard. A light will turn-on in the control unit to give the Presiding officer confirmation of the casted vote.

B. Enhanced Security

• *Pre Armed Check:* Every switch of EVM is important and after turning on the EVM, first thing is to make sure that they are functioning properly. For this issue, a special on board checking system has been introduced which is called Pre Armed Check. In this system, the authority must press every switch to turn on the EVM. If the on board microcontroller detects that all switches are functioning properly, only then the device will be activated for voting.

• *Memory card Error Check:* The device will always check the activity of memory card. If memory card has an error or does not work properly, then the device will give a warning alert. Different memory layer has different warning alert pattern. By hearing warning alert pattern, the faulty memory card layer can be identified instantly.

• *Energy Level Indicator:* The device contains an energy level indicator to get the updates of battery health. The on board microcontroller always read voltage of the battery by using a 10-bit built-in Analog to Digital converter (ADC). Then it shows the value of the battery voltage on a LCD display. The microcontroller also gives a battery low warning alert, when the battery charge goes down below 30% of its capacity.

• *Over enabling indicator and log:* The device will give warning alert if over enabling is occurred. There is an activity log recording system. That's why it is possible to analyze log data and view all the previous activities of this machine if any suspicious incident happens.

• *MCU input surge protection:* Microcontroller input pin will not receive any false trigger during any surge. Every pulse is analyzed and then executed.

• *Device Doctoring Protection:* The device will be automatically deactivated if any one try open it or try to change or modify the functionality of the device.

• *Multiple Memory:* The device has multiple memory layers and all the information are saved into these memory layers. That's why data can be collected from other layers if any one of the memory layers is damaged or does not work properly.

5. COORDINATION OF FRAMEWORK

Coordination of framework is the main part which ensures the secured voting process along with the key button, liquid crystal display (LCD), microcontroller, finger print module, SD card and total processing of the system. [8]

The Arduino Mega 2560 is a microcontroller board based on the ATmega2560. It has 54 digital input/output pins (of which 15 can be used as PWM outputs), 16 analog inputs, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller, simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. GT-511C3 is a small embedded module that consists of an optical sensor mounted on a small circuit board. The optical sensor scans a fingerprint and the microcontroller and software provides the modules functionality which automatically processes the scanned fingerprint. The module itself does all of the heavy lifting behind reading and identifying the fingerprints with an on-board optical sensor and 32-bit CPU. It has an increased memory capacity. The module is small and easy to mount using two mounting tabs on the side of the sensor. The on-board JST-SH connector has four signals: Vcc, GND, Tx, Rx. It can easily store different fingerprints and the database. The LCD display is 128x64 dots and it has blue backlight. [5]

There will be two types of verification system. One is manual verification system and another is FPS (Finger print System) verification. Vote will be allowed if any of this will be successful. All candidates' individual votes will be stored in EEPROM. That's why microcontroller can get the number of votes of all candidates after reboot. We used a buzzer to give some security alert for transparent voting system. There is a Liquid Crystal Display to show guideline messages. It has

one red and one green colored LED to show various events by different presentation. Here, we used a term called "Pre-Armed Check" which helps us to ensure that all buttons are working properly. If any buttons have trouble then the device will not work. There is a SD card to store data that gives extra security for any types of loss of data. There is RTC module to get the actual time. [7]

A. Library reference:

- Fingerprint Library
- EEPROM Library
- Liquid Crystal Display Library
- Software Serial Library
- Serial Peripheral Interface Library
- SD Card Library
- RTC Module Library

B. Global Variable Initialization:

Hardware, External Storage and Communication purposes

- A new text file on SD Card to store records
- Software Serial including fixed Rx and Tx pin
- Liquid Crystal Display including fixed pins
- Fingerprint Module initialization with pins

C. Calculation purposes:

- Individual candidates votes(Integer)
- Total Casted votes(Integer)
- Few boolean variables

D. First Setup

Step 1 :(Initial Setup)

- All types of Serial communication initialization
- LCD Initialization
- Gets time from RTC module
- Power On Fingerprint Module
- All pins mode selection
- On red LED

Step 2 :(Pre-armed Check)

- Checks all the buttons and will continue if everything is ok
- "Pre-armed checks... press all buttons" displays on LCD
- If every button works then displays "Armed Successfully" and goes to Step 3
- Otherwise displays "Check all button.." on LCD

Step 3 :(Startup message)

- Displays "Electronic Voting Machine" on LCD
- Then shows a LED sequence and displays "Starting" on LCD (Blink red and green LED for a few seconds)
- Then displays "Device started" and goes to Step 4.

Step 4 :(SD Card Initialization)

- Displays "SD card initialized" if everything is ok and goes to Step 5.
- Otherwise displays "SD card not initialized"

Step 5 :(Read Vote)

- Reads all candidates individual votes from EEPROM and goes to Step 6.

E. Main Algorithm

Step 6 :(Read Pins)

- Checks current status of all input pins and save these status to boolean variables
- Goes to step 8 if "give_access" pin is high
- Goes to step 7 if "FPS_verify" pin is high
- Goes to step 11 if "Finish" pin is high

Step 7 :(Voter verification)

- Enables FPS module and verify the fingerprint.
- Display "Press Your Finger"
- Goes to step 8 if Fingerprint is matched and displays "Verified Voter"
- Goes to step 6 and give security alert if Finger is not matched.
- If cancel button_pin is high then verification is stopped and goes to Step 6.

Step 8 :(Ask for Vote)

- If any candidate button pin is high then counts relevant candidates vote,
- Shows an LED sequence and goes to Step 9.
- If cancel button pin is high then access is canceled and goes to Step 6.

Step 9 :(Cast Vote)

- Vote will be finalized and red LED will be on
- Save to EEPROM and SD Card
- Access off for vote and goes to Step 6.

Step 10 :(Reset History)

- Erases all candidates votes
- Delete SD Card data
- Replace 0 to EEPROM
- Goes to step 6.

Step 11 :(Finishing process)

- Make the full system off. [9]

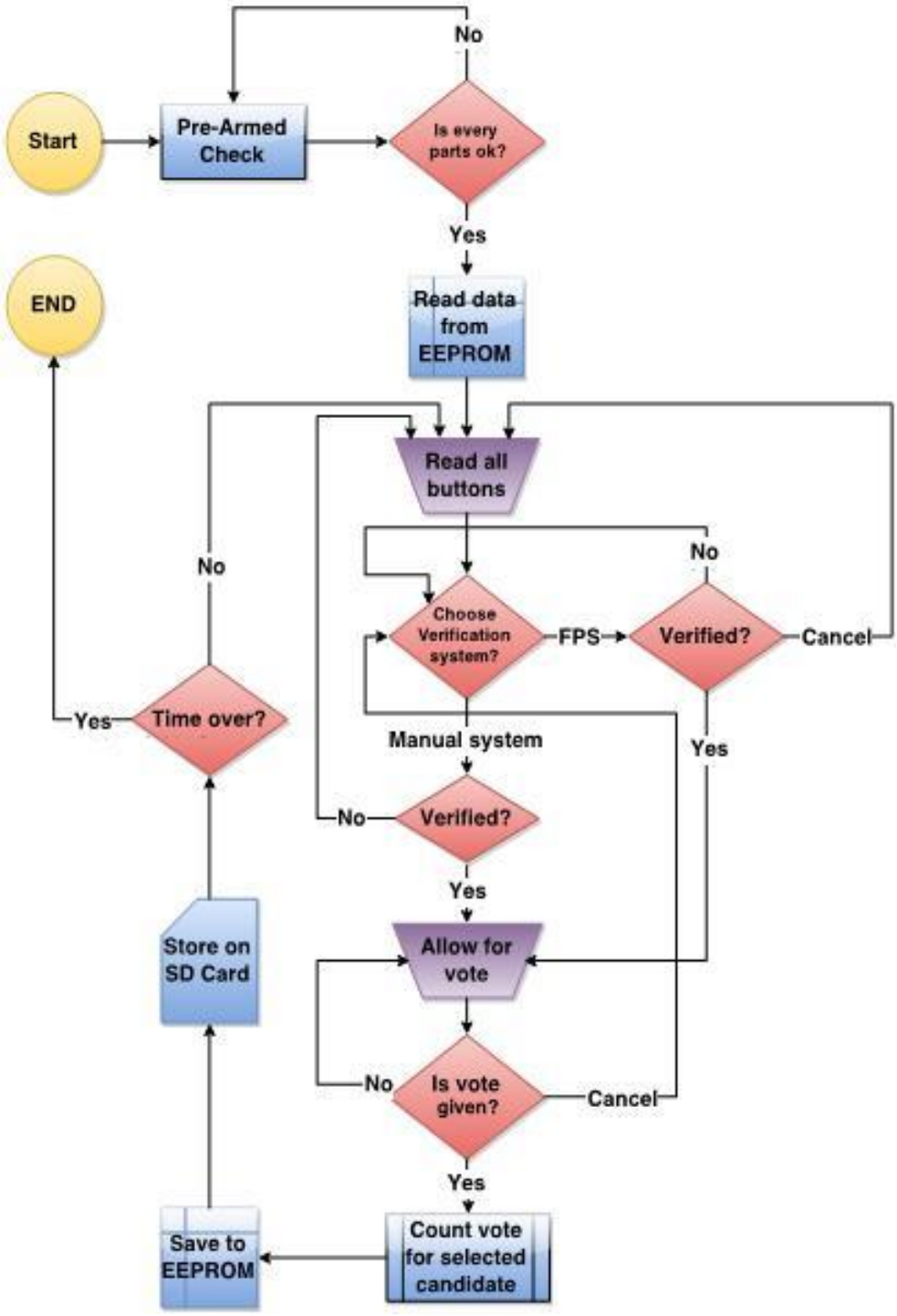

Figure-1: System flowchart

6. SYSTEM IMPLEMENTATION

The proposed framework has been successfully implemented. The steps of total implementation process are shown in the following figures from Figure-2 to Figure-10.

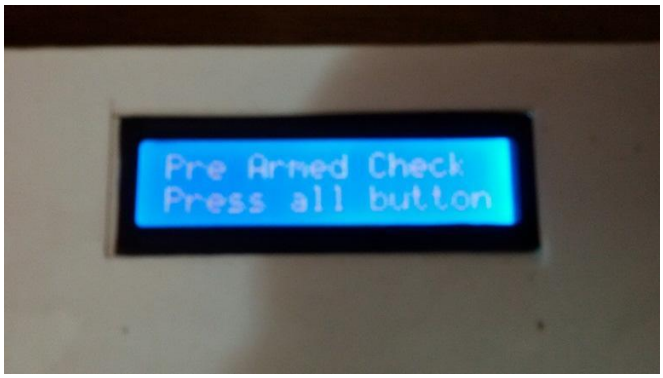

Figure-2: Pre Armed checking starts

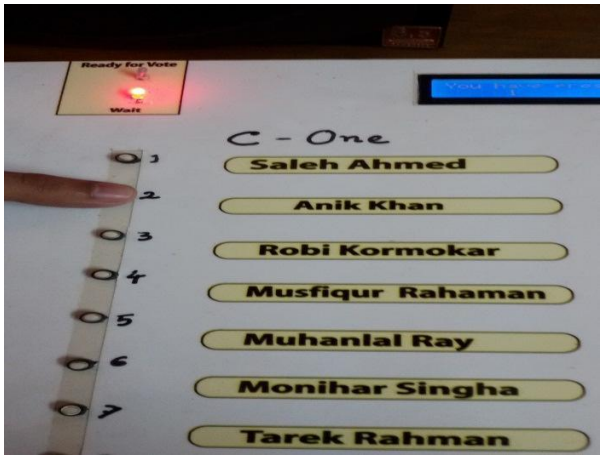

Figure-3: Pre Armed checking continues

Figure-4: Pre Armed checking completed successfully

Figure 5: EVM is starting for voting

Figure-6: Display showing device parameters

Figure-7: Finger print scanning

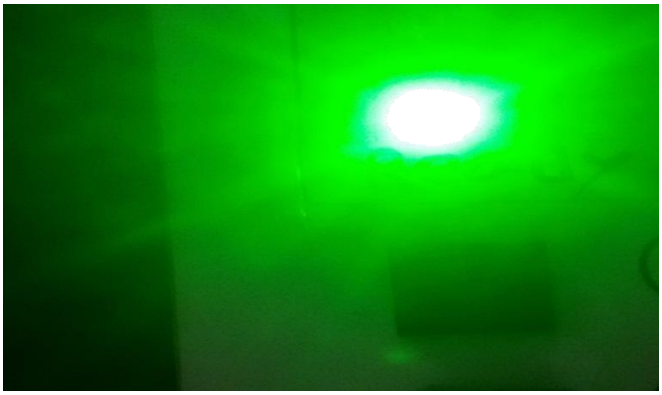

Figure-8: On-board light indicates the presence of a legal voter

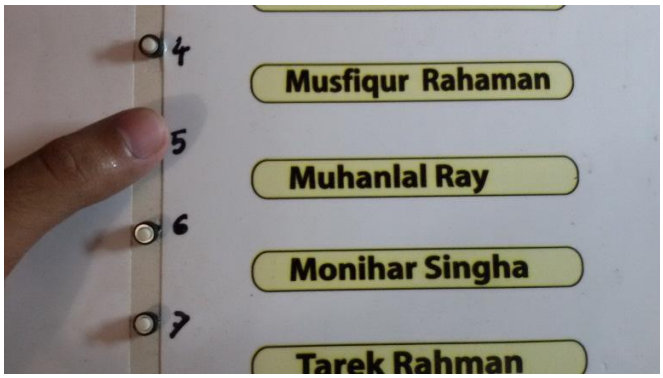

Figure-9: Voter selecting the desired candidate

Figure-10: Display shows the total number of vote casted for each candidate

7. CONCLUSION

The paper turns out to be a vivid manifestation of a transparent voting system which undoubtedly is a better one than the orthodox ballot voting system. The security layers and technology featured in the gadget would surely work as basis for conducting secured e-voting. Voting process with this system overcomes most of the problems faced during the voting period. This will surely ensure a safer voting method which is very much what is required for a healthy voting system of a nation.

REFERENCES

[1] k. Memon, D. Kumar and S. Usman, "Next Generation A secure E-Voting System based On Biometric Fingerprint Method", International Conference on information and Intelligent Computing (IPCSIT), pp.26-32,2011

[2] R. Udupa, G. Garg and P. Sharma, "fast and accurate fingerprint verification", International Conference on Audio and Video-Based Biometric Person Authentication, pp. 192-197,2001.

[3] M. Khan, "Fingerprint biometric-based self-authentication and deniable authentication schemes for the electronic world." IETE Technical Review, vol.26 (3), pp. 191, 2009.

[4] L. O'Gorman, "An overview of fingerprint verification technologies." Information Security Technical Report 3.1, pp.21-32, 1998.

[5] www.arduino.cc.com

[6] Sanjay Kumar1, Manpreet Singh, "Design a Secure Electronic Voting System Using Fingerprint Technique". IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784, www.IJCSI.org

[7] Michael Margolis**,** Arduino Cookbook, Second Edition, O'Reilly publishers.

[8] Massimo Banzi, Getting Started with Arduino, Second Edition, O'Reilly publishers

[9] https://drive.draw.io