

# Anti-Corruption Biometric Voting Machine

<sup>1</sup>Ankita Bhaumik\*, <sup>2</sup>Rana Biswas, <sup>3</sup>Shamik Chakrabarty

<sup>1</sup>Department of Computer Science and Engineering, University of Calcutta

<sup>2</sup>Department of Computer Science, St. Xavier's College, Kolkata

<sup>3</sup>School of Computer and Information Sciences, Hyderabad Central University

## Abstract—

The primary requirement of any democratic government or institution is a fair voting system. But corruption is prevalent in almost every corner of the world today. The main shortcoming of an electronic voting machine (EVM) is its inability to distinguish the voters. Hence one voter may cast a vote multiple number of votes and there is no mechanical or technological means to stop such a thing. Also, a person may cast a vote on behalf of sum one else creating duplicity and corruption within the entire process. As a result people abstain from voting for the deserving candidate. An anti-corruption biometric voting machine distinguishes voters on the basis of their registered fingerprint and allows them to vote only once.

**Keywords—**Anti-corruption, Arduino Uno, Biometric, Fingerprint Module, Voting Machine

## I. INTRODUCTION

A “biometric voting machine” uses the unique feature i.e. fingerprint, present in every human being to enable him to cast a vote only once. The main motivation behind this system is to effectively manage the voting process in a democratic institution without the inclusion of corruption or any unfair means [4]. A voter registers himself into the database with his fingerprint. Then the person can only cast his vote if he has been previously registered. A voter is also restricted from casting more than the permissible number of votes. If any voter does so, an alarm is raised by the system. This voting machine serves two purposes:

- A person cannot vote more than once.
- A person cannot vote on behalf of sum one else.

Hence our project is aimed to remove corruption at the very basic level [5] thus contributing to the development of the country/institution [2]. A fair voting system will help bring into power the true leader that the majority supports and not someone who resorts to unfair and unjust means [3].

## II. SYSTEM COMPONENTS

The user registers his/her fingerprint at the fingerprint module. The fingerprint module reads the fingerprint and based on the choice of the user, it will register, or cast a vote or display the results [1]. If a user chooses to register, his fingerprint will be registered into the database only if he has not registered before. If the user chooses to vote, he can cast a vote only if he has not voted before. If he has voted before then an alarm will be set to inform the authorities [6]. If the user chooses to view results, his fingerprint will be matched with the fingerprint of the person authorized to view the results. If a correct match is found then the results will be displayed otherwise the alarm will be set to notify the authorities [7].

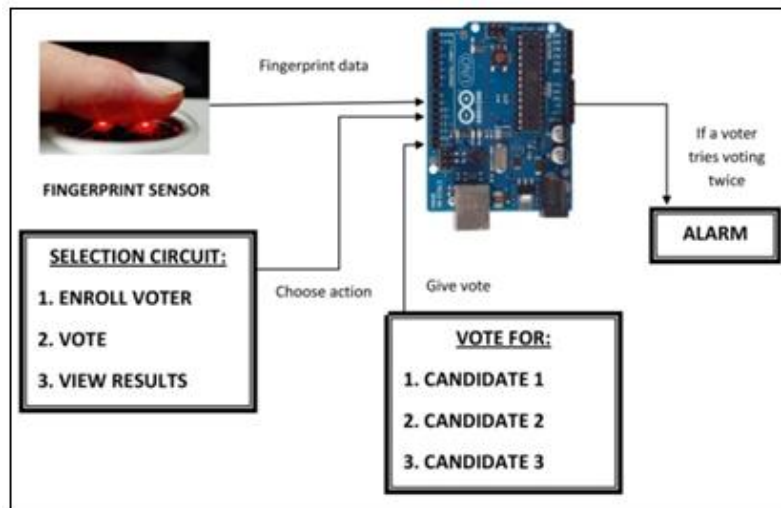


Fig 1: Block diagram of the system

The circuit components are as follows:

**A. Fingerprint Module R-305:**

It receives the fingerprint of the voter. This is a finger print sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter [10]. It scans and reads the fingerprint and send the data to the Arduino Uno.

**B. Arduino Uno microcontroller:**

It does the programming and checking required for processing the fingerprint using Arduino Sketch. The Arduino Uno [8] is a microcontroller board based on the ATmega328 [9]. It receives data from the fingerprint module via the serial input pin and processes the data. Depending on other external inputs, it performs the voting process.

**C. LCD:**

It displays various messages to the voter about the voting process.

**D. Switching Circuit:**

The switching circuit is used to take into account the various choices made by the user. It selects the choice of the user and does the appropriate functions. It consists of several switches which when pressed sends a high signal to the arduino circuit and does the respective functions. The switches represent the various choices of enrolling, voting, showing results as well as the list of candidates.

**E. Alarm:**

The alarm is used to raise an alert in case of corrupt activities. It is connected to the arduino circuit. If a person votes more than the permissible number of times or if an unauthorized person tries to check the results, the alarm is switched on and the authorities in charge are informed.

**III. SYSTEM IMPLEMENTATION**

The various steps in the voting procedure have been listed below. It is to be noted that the phases described need not be executed at the same time. Normally, the enrolment phase is performed first. Following the enrolment phase is the voting phase and finally the results phase.

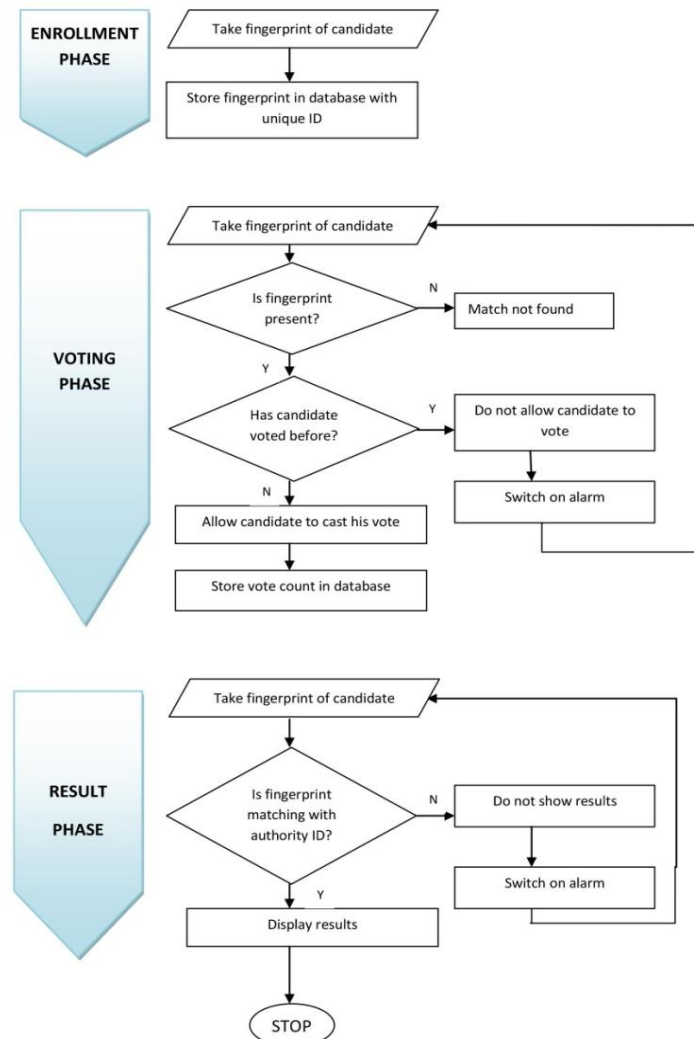


Fig 2: Flowchart

**A. Enrollment Phase:**

Step 1: Take fingerprint of candidate.

Step 2: If fingerprint not present, store it into database and assign a unique ID.

Step 3: If fingerprint present, display message indicating enrollment being previously done.

**B. Voting Phase:**

Step 1: Take fingerprint of candidate.

Step 2: If fingerprint is not present in database, display message to show the candidate is not enrolled.

Step 3: If fingerprint is present in database, check whether the candidate has voted for less than the permissible number of times.

Step 4: If candidate has voted already for the permissible number of times, switch on the alarm indicating fraud voter.

Step 5: If candidate has not voted for the permissible number of times, allow him to cast a vote and store vote count into the database.

**C. Result Phase:**

Step 1: Take fingerprint of candidate.

Step 2: If fingerprint ID matches with the Voting Authority ID, display results.

Step3: If fingerprint ID does not match the Voting Authority ID, then switch on the alarm indicating attempt for unauthorized viewing of results.

**IV. MACHINE IMPLEMENTATION**

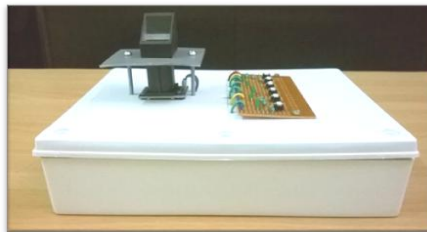


Fig 3: Anti -corruption biometric voting machine

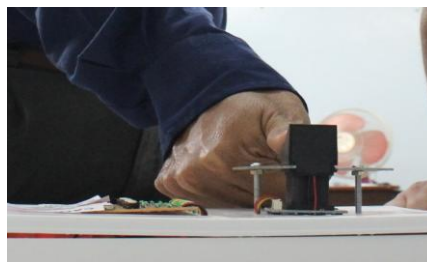


Fig 4: A candidate registering his fingerprint

**V. CONCLUSION**

A biometric voting machine can be used to remove corruption at the very basic level of any democratic nation. As opposed to the present EVMs used in India, the biometric voting machine is priced much less and with mass production will be even lesser. Hence, it will save a lot of the national treasury which can be used to improve the nation in turn. It can be used in all form of election procedures, be it in forming the government of the nation or the local municipal bodies.

As technology promises to make our lives better, we have used technology to remove the utmost evil prevalent in the society- corruption. It is our duty as citizens of this world to remove corruption at once, and this responsibility has caused us to develop this project.

**REFERENCES**

- [1] S. Gaur, V.A. Shah, M. Thakker, "Biometric Recognition Techniques: A Review", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 1, Issue 4, Oct. 2012. ISSN 2278 – 8875.
- [2] J. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?" *Proceedings of the IEEE*, Volume: 85, Issue 9, pp. 1480 – 1492, 1997.
- [3] K.A. Gbolagade, M.O. Yinyeh, "Overview of Biometric Electronic Voting System in Ghana", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 7, Jul. 2013 ISSN: 2277 128X.
- [4] R. Ghadge, M. Patil, V. Pimplodkar, V. Vibhute, A.R. Zade, "A Survey on Voting System Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 1, Jan. 2013, ISSN: 2277 128X.

- [5] N. Kakhandaki, A. Konnur, A. Nandibewoor, “Preferential Electronic Voting Machine - An Embedded Computing Solution”, *Journal of Emerging Technology and Advanced Engineering*, Volume 3, Issue 3, Mar. 2013, ISSN 2250-2459.
- [6] T.U.S. Begum, D.A. Kumar, “A Novel design of Electronic Voting System Using Fingerprint”, *International Journal Of Innovative Technology & Creative Engineering*, Volume 1, Jan. 2011, Issn: 2045-8711.
- [7] R. Alaguvel, G. Gnanavel, K. Jagadhambal, “Biometrics using Electronic Voting System with Embedded Security”, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, Volume 2, Issue 3, Mar. 2013, ISSN: 2278 – 1323.
- [8] Arduino homepage on Arduino Uno [online]. Available: <http://arduino.cc/en/Main/arduinoBoardUno>
- [9] “Atmega328 datasheet”, [online]. Available: <http://www.atmel.in/Images/doc7810.pdf>
- [10] Sunrom Electronics/Technologies homepage on Finger Print Sensor(R305) [online]. Available: <http://www.sunrom.com/p/finger-print-sensor-r305>