Implementation of Secure E-Voting System

Neha Bansod[1], Mitali Shegokar[2], Kunal Kore[3] , Prof. Mrs. Komal S Vyas[4]

[1]Neha Bansod , ENTC, SSGMCE, Shegaon
[2] Mitali Shegokar, ENTC, SSGMCE, Shegaon
[3] Kunal Kore , ENTC, SSGMCE, Shegaon
[4]Komal S Vyas , ENTC, Prof. at SSGMCE, Shegaon

---***---

ABSTRACT:

India is a democratic nation that is home to many diverse religions, dialects, and cultural traditions. Every citizen has the right to vote in order to choose their government's chief executive. The current structure makes it incredibly difficult and expensive to conduct elections nationwide, and it also requires a lot of manpower. Elections can be held fairly with the suggested method because it requires less labour. Voter identification using personal information is made possible by new voting procedures. Every voter's biometric thumb impression is collected and stored there. When it comes to elections, each voter's thumb impression is compared to the data and, if deemed accurate, he is granted the opportunity to vote.

Index Terms: Arduino, voter, and fingerprint scanning

1. INTRODUCTION

Rigging, or when one person casts numerous votes, is the most serious and common issue encountered when holding elections. However, an ink mark is placed on the voter's finger to identify those who have already cast their ballot. However, there are numerous ways to simply remove that ink mark, which increases the likelihood of fraudulent voting. To address the rigging issue mentioned above, we suggest creating a revolutionary biometric-based voting architecture through this research. The Finger Print Sensor Module is an apparatus that reads a fingerprint's scanned picture, converts it into a digital code, and then saves the code in memory. The entire procedure is controlled by the Arduino microcontroller. Additionally, it lessens the possibility of mistakes, increasing the process's security and dependability.

2. USEFULNESS

• Corrupt officials are unable to tamper with the voting process.

• It is possible to prevent the impersonation of absentee voters in order to skew the results in favour of one candidate.

• Voter identity and eligibility are recognized.

Technology advances have made misconduct and outcomes controversy more challenging.

• No one may cast more than one ballot, and if they do, they must abstain and notify the authorities.

• Voting illegally under a false name can be prevented.

• Increases the voting process's dependability.

• It assures that the voter is who they say they are.

By assuring a fair process for gathering and tallying the votes, the public's faith in democracy is preserved. Additionally, voter data is retained in a more secure environment.

3. LITERATURE REVIEW

A voting method that relies primarily on paper work and uses a basic electrical equipment was described by Kumar and Begum [1]. A significant amount of administrative effort is included to protect the information of voters who must carry voter ID cards to the polling place for validation. Voters use electronic voting machines to cast their ballots after the election official has verified them. The voting machine has a list of all the candidates running for office, and the voter can select the candidate they want to support by selecting the proper button. It is necessary to think about digital advances and their security in order to overcome this traditional electoral framework. J. Deepika, S. Kalaiselvi, S. Mahalakshmi, and S. Agne Shifani [2] It has to do with the idea of taking a voter's fingerprint, which is then submitted into the system. Then compared to the database's data that is currently available. Voting rights are made available if the specific pattern matches anyone on the records that are readily available. The outcome is then immediate, and IOT is used for the counting. V. Likhitha, G. Rama Lakshmi, K.V. Renuka, T. Alekhya, and CH. Sri Rekha [3] The Raspberry Pi has a Python program me that interfaces with a keyboard and a fingerprint sensor. The voter's information is kept in the database on the raspberry pi, enabling processing of the voter's fingerprint input. The output will then be presented in the LCD as the voter presses the keypad to cast his or her ballot. Ganesh Prabhu S, P. Jayarajan, and R.R. Thirrunavukkarasu [4] Through two-step authentication employing a facial recognition and OTP system, the user can cast a remote ballot from any location using a computer or mobile device, obviating the need for them to physically travel to the polling place. If the user feels more comfortable doing so, it also gives them the option to vote offline. The face scanning system is used to capture images of voters' faces before the election and is helpful when casting a ballot. Instead of voter identification, the offline voting method is improved with the use of RFID tags.

Kumaresan Perumal and Ramya G [5] We can spend our time as we like and cast our votes online from any location. This was accomplished using C# as a programming language, Microsoft SQL Server 2012, and Microsoft Azure as a cloud. Prof. Rohini, Ms. Ashwini Ashok Mandavkar Agawane, Vijay [6] In which it takes pictures of the voters' faces and compares them to pictures already in the database. The OTP (One-Time Password) is produced and sent to the registered mobile number of the voters after the validity of the facial detection is confirmed. Once the voter has been verified, he may cast his ballot. This method of voter verification is highly quick and efficient.

4. METHODOLOGY

In the current study, it is suggested that the EVM system employ a finger print reader to use voters' biometrics to check their legitimacy. The process's overall block diagram. here are five pushbuttons There have been uses for Delete/Okay, Check Match, Register/Back, Move Up, and Move Down. The keys Register and Delete have two functions. The two functions of the Register key are fresh enrollment and going back functionality. The Aadhaar ID can be used to complete this process on the original devices. The voter must first touch the register key before entering their ID to register. The entire process cycle is directed by LCD. Now, if the user wants to cancel the procedure at this point, he or she can return by repeatedly pressing the Register (Back) key. The user can enroll new fingerprints by using the up and down arrow buttons simultaneously. Pressing the okay key will allow us to move forward, and pressing the delete key will allow us to remove any earlier impressions that are no longer relevant. The Match key's objective is to validate the voter's eligibility. The user is permitted to cast his vote if the fingerprint is identical to the print stored in the database.

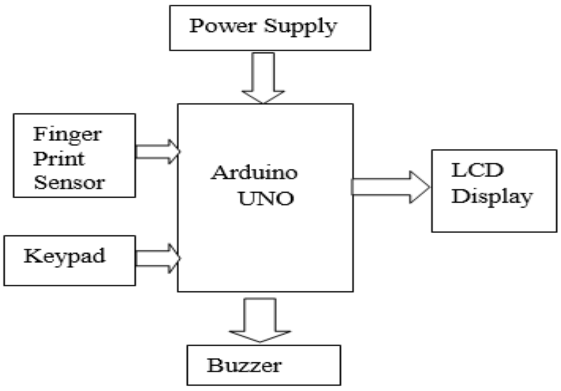

Fig. 1 Block diagram of Implementation of Secure E-Voting System.

The module transforms a fingerprint scan into a digital template with hills (represented by 1s) and valleys (represented by 0s) using the fingerprint's scanned image. The voting procedure begins if the authenticity is confirmed. The voter receives a list of the candidates running for office. He or she chooses a candidate by hitting the button next to the candidate's name, and the vote total is added to the framework. The LCD prompts the user to maintain finger contact with the fingerprint sensor. The LCD displays "voter authorized" when the module has captured the image. The voter is then able to select their preferred candidate. By pressing a fresh set of matrix keys, this is accomplished. Currently, if a previous voter returns and needs to cast a vote again, the system will show "Already Voted" at that time.

5. HARDWARE INFORMATION

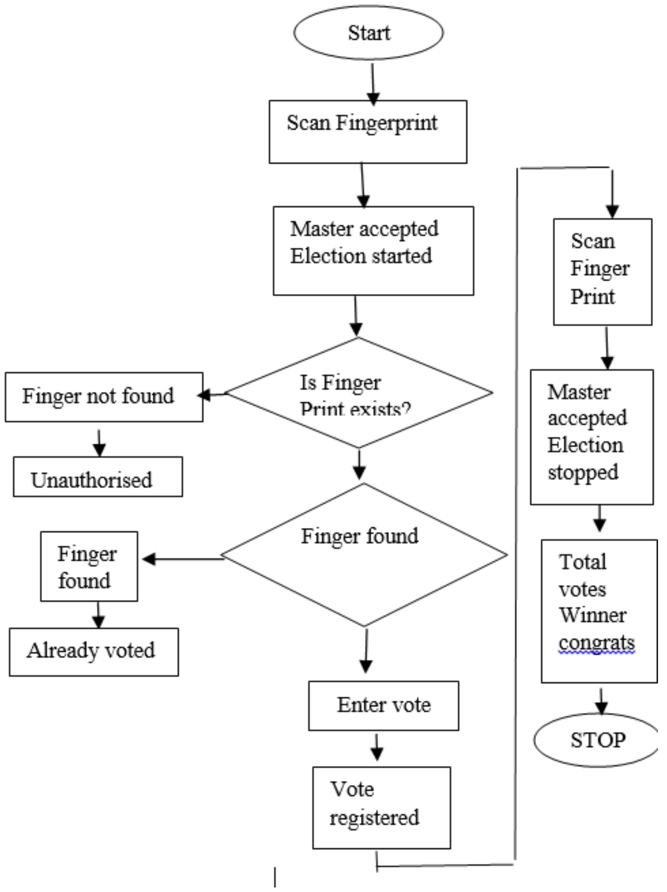

Fig. 2 Flowchart of the proposed project.

Uno Arduino

Popular microcontroller boards include the Arduino Uno, which is used by professionals, academics, and amateurs alike. It can be applied to a wide range of projects, including data logging, robotics, and home automation. Based on the ATmega328P is a microcontroller board known as Arduino Uno. It contains a USB port, a power jack, an ICSP header, six analogue inputs, fourteen digital input/output pins, six of which can be used as PWM outputs, a 16 MHz quartz crystal, and a reset button.LCD Display An alphanumeric display module with 16 characters and 2 lines is known as a 16x2 LCD (Liquid Crystal Display). It is frequently employed in a variety of electrical applications for the display of data like temperature, time, and messages. Sensor for fingerprints: The R370 fingerprint sensor uses optical sensing technology as its sensing medium. Images taken by the R370 sensor have a 256 × 360-pixel resolution. working Temperature: The working temperature range for the R370 fingerprint sensor is -10°C to +55°C.The R370 fingerprint sensor's false acceptance rate (FAR) is 0.001%. The R370 fingerprint sensor's false rejection rate (FRR) is 0.1%. Data communication for the R370 fingerprint sensor takes place over a USB 2.0 interface. electricity Requirements: The R370 fingerprint sensor requires 170mA of electricity at 5V DC. Up to 10,000 fingerprint templates can be stored in the memory of the R370 fingerprint sensor. Windows, Linux, and Android operating systems are all compatible with the R370 fingerprint sensor.

6. CIRCULAR ECONOMY AND ITS OPERATING PRINCIPLE

The fingerprint-based voting machine's suggested circuit includes an Arduino for overall process control. The Arduino microcontroller is used to operate the registration links for new users, voter ID selection, and voting procedures, as well as an alert buzzer, a pair of LEDs and a voter-facing 16x2 LCD instructions and election results. The proposed circuitry's schematic diagram is shown in Figure 4. The fingerprint module's Transmitter (T1) and Receiver (R1) sections are each directly linked to the serial pins T1 and R1 of the Arduino microcontroller. The module is driven by a 5V supply that is taken from the Arduino board.

The Arduino is used in the proposed voting machine circuit to control every step of the voting process. The Arduino microcontroller is used to operate the push buttons for new registrations, voter ID selection, and voting procedures, as well as an alert buzzer, a set of LEDs, and a 16x2 LCD for voter instructions and election results. The proposed circuitry's schematic diagram is shown in Figure 4. The fingerprint module's Transmitter (T1) and Receiver (R1) sections are each directly linked to the serial pins T1 and R1 of the Arduino microcontroller. The module is driven by a 5V supply that is derived from the Arduino board.

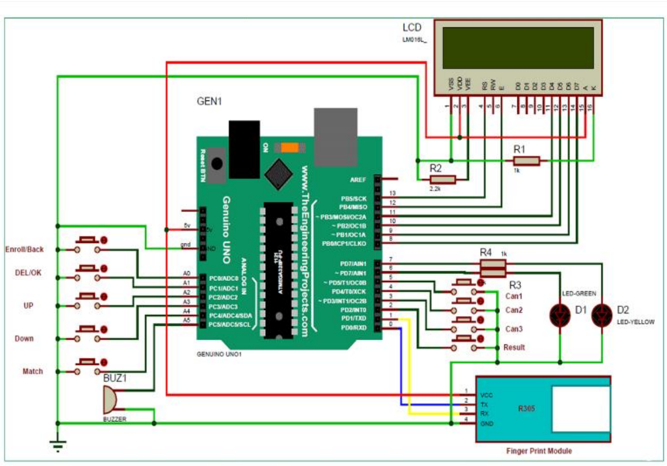

Fig. 3 shows a circuit and how it functions.

The Arduino's pins D5 (Candidate1), D6 (Candidate2), D3 (Candidate3), and D2 (Outcome) are all directly linked to the push buttons with regard to the ground. The Arduino pins A0 (Register), A1 (Delete and OK), A2, A3, and D4 (Check Match) are also all connected to the push buttons. Digital pins D7, D6, D5, D4, EN, and RS of a 16x2 LCD that is set up in 4-bit mode are connected to the Arduino's digital pins D8, D9, D10, D11, D12, and D13, respectively. The Arduino is coded such that when a voter arrives to cast his vote, it is first checked to see if his fingerprint matches any previously saved fingerprints of individuals who have already cast their votes. Only the voter will then be permitted to cast his or her vote Every time a voter casts a ballot, his distinct finger impression is also recorded and stored on a remote computer. If the same person votes twice, the number pad won't be functional, either voluntarily or accidentally due to the synchronisation of the distinct finger impression with previously saved fingerprints. A high level of security will be upheld if voting fraud and other forms of vote tampering are avoided. Additionally, before casting a ballot, the machine will verify that the voter by comparing his finger print to one that already exists in the database, is recorded with the Election Commission database, preventing voter fraud. Therefore, the entire election procedure might be changed to include biometric authentication prior to casting a ballot, by a voter. ensuring fair and unbiased elections.

7. RESULTS

Only the authorized voter can access the constructed biometric-based EVM, which has been tested for all of its features and found to operate quite accurately. Any user can use the system, even if he is unfamiliar with all of its details.

8. CONCLUSION

As electronic voting machines progress, this paper is utilized to conduct efficient, secure, and corrupt-free elections, hence boosting public confidence in the electoral process. The system can help the electoral commission with security and manpower difficulties.

REFERENCES

[1] *D. Ashok Kumar#1, T. Ummal Sariba Begum#2, “A Novel design of Electronic Voting System* Using *Fingerprint”. INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING (ISSN:2045-8711) VOL.1 NO.1 JANUARY 20001*

[2] *1 J.Deepika , 2 S.Kalaiselvi ,3 S.Mahalakshmi, 4 S.Agnes Shifani, “Smart Electronic Voting System Based On Biometric*

Identification-Survey". 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)

[3] *G.Rama Lakshmi, V.Likhitha, K.V.Renuka, CH.Sri Rekha,T.Alekhya "E-Voting System using Biometrics". Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS 2019) IEEE Xplore Part Number: CFP19K34-ART; ISBN: 978-1-5386-8113-8*

[4] *Ganesh Prabhu S, Prabu.S, R.R.Thirrunavukkarasu, Nizarahammed.A, Raghul.S, P. Jayarajan, "Smart Online Voting System". 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)Y.*

[5] *Ramya G, Kumaresan Perumal, K.Sree harshitha "Online Voting System using Cloud". 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE).*

[6] *Ms.Ashwini Ashok Mandavkar, Prof. Rohini Vijay Agawane. "Mobile Based Facial Recognition Using OTP Verification for Voting System" 2015 IEEE.*

[7] *Mendu Vaishnavi, Tejasree Kaka, Duvvuri Sai Suma, K. Sriram. " International Journal of Engineering Research & Technology (IJERT) Vol. 9 Issue 09, September-2020.*

[8] *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.*

[9] *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.*