BIOMETRIC IDENTITY AND IOT-BASED ELECTRONIC VOTING MACHINE

Dr. Shalini Shravan
Dept. of ECE,
RV Institute of Technology and Management
Bengaluru, India
shalinishravan.rvitm@rvei.edu.in

Kathe Sai Sreenivas
Dept. of ECE,
RV Institute of Technology and Management
Bengaluru, India
kathesais_ec19.rvitm@rvei.edu.in

R K Lasreeth Kumar
Dept. of ECE,
RV Institute of Technology and Management
Bengaluru, India
lasreethrk_ec19.rvitm@rvei.edu.in

Veeram Lohith Kumar Reddy
Dept. of ECE,
RV Institute of Technology and Management
Bengaluru, India
veeramlohithkr_ec19.rvitm@rvei.edu.in

Kuruva Dheeraj
Dept. of ECE,
RV Institute of Technology and Management
Bengaluru, India
kuruvadheeraj_ec19.rvitm@rvei.edu.in

***Abstract*— The election is a process in which the people will have a right called the vote to choose the government. The elections play a crucial role in the development of the country. Every citizen of the country will feel proven to cast their votes during elections. The government has to conduct fair elections. This paper is about an IOT (Internet of Things) based electronic voting machine with a fingerprint module for authentication. In this paper, we are focusing on the voting phase. We have worked on a voting machine that works with the help of a fingerprint module and is based on IOT (Internet of Things). Fingerprint module which will help check whether he is an authorized person. There will be two distinct phases to the proposed work's operation. The user's authentication is one thing, while the authorized person's casting of votes is another. Fingerprint authentication will be used during the process of authentication. All voter's fingerprint databases are originally saved in the system as a requirement. While evaluating the equipment, we obtained precise results. Any person who wishes to cast a ballot for any party must first pass a fingerprint authentication process. A successful fingerprint match allows the voter to select whatever party they choose. Data on the proportion of the vote for each party will be used for the analysis of data. The system provides an alert on malpractice and allows only an authorized voter to cast the vote. We have reviewed the paper which worked on the development of EVM (Electronic Voting Machine).**

Keywords*— *IOT (Internet of Things), fingerprint, Authentication process, Analysis of data, EVM (Electronic Voting Machine, casting of votes.

I. INTRODUCTION

Democracy is the law in India. Voting is an important way for citizens to exercise their constitutional right to vote in a democracy like India. Voters commonly cast their ballots in a polling place. As technology develops, electronic voting machines continue to be used to cast votes. The Election Commission of India, in partnership with Bharat Electronics Limited (BEL) and Electronics Corporation of India Limited, developed the Indian electronic voting machine (EVM) in 1989. (ECIL). Since 2004, all national and state legislature elections in India have been performed with electronic voting machines. Only 31 of the 120 democratic countries rely on voting by electronic machines, either regionally or nationwide. Other countries continue to utilize ballots made of paper as they don't trust electronic voting machines. Several situations which have come to the Supreme Court of India that is now pending [8] demonstrate the safety of this EVM. The voting technique and the functioning of the voting machine are not clear to the voter.

Voting and democracy go hand in hand, it is acceptable to believe. Our main goal is to allow as many eligible voters as are able to take part in the process of voting. Since 2004, electronic voting machines (EVMs) have occupied the place of paper ballots and people vote counting in India's electoral system. The government makes all it can to teach the general public about the significance of voting, but for a wide range of reasons, a few individuals might not be able to make use of their right to vote [1].

Practically every sector has experienced major modifications because of technology, and elections are no different. Technology is utilized by individuals to simplify their work simple, speedy, and reliable. Even though the traditional paper ballot voting procedure is uncomplicated, it is not clear or error-free. Authenticated System Of voting is used to bypass the disadvantages associated with conventional paper-based ballots [11].

Voting's primary objective is to offer voters the opportunity to exercise their freedom of expression by expressing their opinions on particular issues, regulations, public movements, constitutional amendments, recalls, and/or presidential candidates. Technology is progressively utilized to help voters vote in elections [4]. Voter identification is needed twice during the election process: first, at registering to vote to acquire the right to vote; and secondly, during voting to allow a citizen to utilize their right by verifying that perhaps the person meets all requirements to vote (authentication).

The voters are losing their votes during the election process due to voting rigging. Vote rigging is a process in which the unauthorized will cast the vote and the authorized person will lose the chance of voting. Due to the process of vote rigging, the voters are losing their trust in elections. To secure the voting process, we must use updated technology to ensure that elections are conducted lawfully. This work aims to build a system that will stop Vote rigging and helps remove electoral fraud that may lead to injustice in the election process.

The Internet of Things (IoT) is the ability for devices to connect to one another through the web or other networks, tracking data remotely, giving feedback, and assisting in judgment for business, industry, and home uses [5]. Typically, sensors connected to something like a back-to-base system are used for this. The term "Internet of Things" (IoT) refers to physical items equipped with sensors, computing power, software, and other technologies that communicate with each other and exchange data through the Internet or even other communications systems.

For the purpose of verifying voter fingerprints, we will employ pattern-based (image-based) matching and correlation-based matching methodologies. Pattern-based (or image-based) matching compares the fundamental markings (arche, spiral, and loops)

between a candidate's fingerprint and a previously stored template. The photos must be oriented in the same direction in order for this to work. Correlation-based matching involves superimposing two fingerprint pictures and computing the correlation among pixel locations for various alignments.

II. LITERATURE SURVEY

This survey of the literature intends to shed light on the many implementations and concepts linked to this area as well as the ones that have benefited in the conception of the thought.

Suraj HP [1] has proposed an IOT-Based Remote Electronic Voting System Using Aadhar and Dual Biometric Authentication that uses biometrics and face recognition. The current electoral system has flaws and calls for an enormous amount of manpower. We have dual biometric security, which entails a fingerprint scanner accompanied by machine vision, to increase safety and allow clean polling. The system's limitation is that it's quite hard to recognize a human personality. Face detection might trigger the system to stutter.

G.Nithya [2] has implemented a fingerprint-based electronic voting machine using Arduino. Electronic voting machine using fingerprints, The Arduino Uno is indeed the microcontroller employed in the project. The person's fingerprints are used to confirm their identity. Everyone else's fingerprints vary from each other at least a tiny bit. When fraud occurs, the message "Already voted" will appear. The board is programmed via the Arduino IDE, and ballot cards are displayed. Always an authorized voter can cast a vote, as well as the system provides a warning in the case of fraud. The absence of information storage is one of this project's limitations.

Miral Desai [3] has worked on an Internet of Things (IoT)-Based Advanced Voting Machine System Enhanced Using Low-Cost IoT Embedded Devices and a Cloud Platform. This article discusses the creation of an IoT-based, efficient, and secure voting system that is electronic. The recommended solution trumps the two current infrastructures since they both need a lot of time and are not verified. The suggested system includes two various stages that everything goes through. User polling and authentication mechanisms are two examples. Fingerprint recognition is a way to authenticate. In the initial step, the system can store a fingerprint image of each and every voter.

Abeesh A I [4] has worked on Electronic Voting Machine Authentication using Biometric Information. This report's structure allows most of the PIC16F877A microcontroller in conjunction with associated accessories including one with a GSM modem, a fingerprint reader, and a Display. Users can also access a subscriber geography graphical interface to vote for a candidate after passing the verification procedure. The polling technique is efficient, rapid, and confidential since the votes will indeed be instantly processed. The GSM connection provides the voter with immediate feedback right after they have voted.

Shilpa C Venugopal [5] has implemented IOT based voting machine with fingerprint verification. This is one of the existing approaches. Accessing the voter's fingerprint may indeed be performed underneath the existing arrangement. Immediately afterward it's going to be matched to the inner detection algorithm. The fingerprint module on Arduino can be utilized to implement an IOT-based voting machine with fingerprint verification. Nonetheless, the downside with this sort of system is that we're incapable to store the voting set of data on the domain controller.

Sharathchandra N R [6] has implemented IOT Based Fingerprint Voting System. This is a proposal designed to entirely eliminate manipulation. BIOMETRICS means "knowledge of life" in ancient Greek writing. Fingerprint, face, iris, voice, signature, and hand geometry recognition and verification are popular biometrics research. The machine scans and matches his biometric picture with a previously recorded image. If both photographs agree, the individual is allowed to vote in the election. If indeed the fingerprints were not linked, the buzzing would ring a warning, but also that individual wouldn't be able to participate. We may prevent manipulating this manner. When the polling is completed, use the "results" option to obtain the final outcome.

Sushil Kumar Singh [7] has proposed an Internet of Things Based Electronic Voting Machine. The Internet of Things Based Electronic Voting Machine is research that deals with how, as technology advances, the Internet has become an integral aspect of our life. The Electronic Voting Machine (EVM) utilizing IoT is presented in this study. As the election process must be equitable and open, fingerprint-based EVMs may be one of the options. The study focuses on the notion of an online voting process for elections, in which voting information is quickly transmitted and a mechanism is in place for tracking a proxy vote. Field testing was carried out to assess the effectiveness of the suggested system and to construct a hardware model.

Arun Kumar S [8] has worked on the IoT-based EVM. This EVM has a scanner that reads QR codes for scanning the QR code on the voter's AADHAR card. The Barcode is used to retrieve voter information such as fingerprints and names from the Aadhaar - based Database. During the voting process, this information is compared to the fingerprint collected using a Biometric sensor. The vote is only counted when the voter has been validated. This eliminates fraudulent voting and ensures that just the voter submits the vote. When the relevant key to show the program is clicked, the EVM gives clarity by showing the complete program operating within the machine. This EVM does not require a control unit because all functionalities are integrated into a single device.

III. PROPOSED SYSTEM

This project is developed to detect voting rigging and to conduct a fraud-free election. We have developed an IoT device i.e., an electronic voting machine that will use the fingerprint to authenticate. The person who will be casting their vote must first verify their fingerprint which is unique for all. The fingerprint of a person will not match with others. So, we have used the fingerprint as the unique identification of a person.

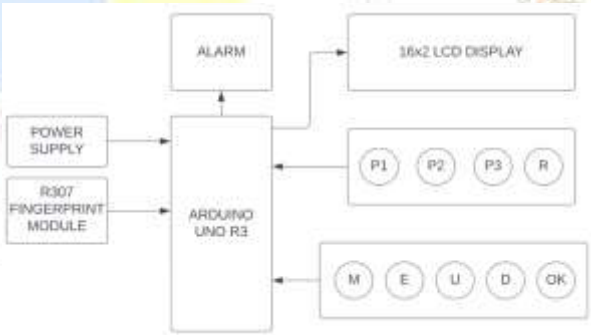

Fig.1: Shows the design of the model.

Fingerprint verification can also be a trustworthy option for e-voting systems if users are well-informed and trained, and the system runs in a controlled environment. Because of the comparably inexpensive price tag, small dimensions, and ease of integration of fingerprint recognition devices, the personal computer access application field looks to be practically solely based on fingerprints. Capture the finger vein picture and compare or match it to the database. A match between the capture finger veins and the record fingers vein shows that this individual is eligible for the polling section and that the criterion is met automatically.

A. System Working

We have developed the framework such that it is easy to use. The power supply for this gadget comprises a 0-9v adapter. We have used Arduino Uno as the microcontroller. We have used the 16X2 LCD display for knowing the process that is been carried out.

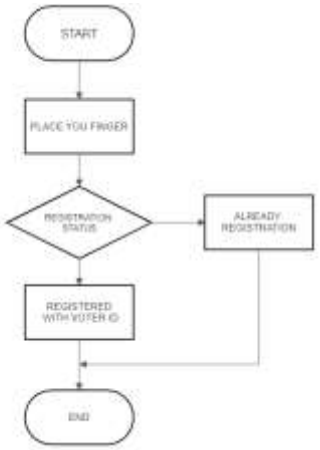

Fig.2: Flow chart of the fingerprint registration process.

we have used the R307 Fingerprint module that will help to check the fingerprint authentication of the user. A warning signal is employed to notify the approved people regarding the EVM (Electronic voting machine) scam. We have preserved a variety of options that will assist people in enrolling and voting.

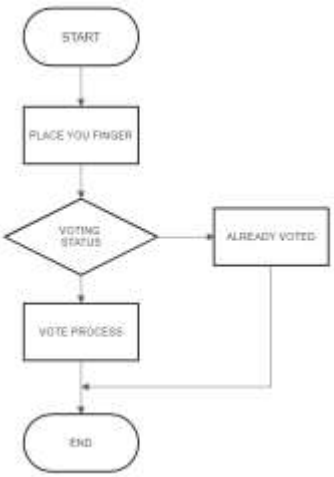

Fig.3: Flow chart of the vote-casting process.

B. Working Principle

The functioning of an optical fingerprint scanner (TIR) is based on the concept of total internal reflection. To allow TIR, an optical fingerprint scanner employs a glass prism. A precise angle of LED illumination (typically green in color) must be allowed to travel through a single side of something like a prism to generate TIR. All of the reflecting surfaces exit via the prism's other face, which houses lenses and an imaging system (essentially a camera). When no finger is placed on the prism, all of the light bounces through it, providing the image sensor with a plain image. The Evanescent Wave is a little amount of light that escapes and is present in the outside environment during TIR.

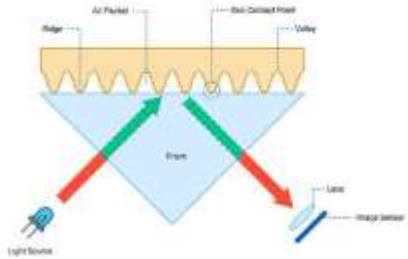

Fig.5: Working of R307 fingerprint module [13]

IV. RESULTS OF IMPLEMENTATION

Whenever the voter places his or her enrolled fingertip in the scanning device, the system compares it to the pre-stored imprint in the database. If it is displayed, the machine will let the voter vote by activating the voting unit. Otherwise, the procedure is terminated since the fingerprint is not matched.

First, it will show you "Press the match key to start the system". To enroll the finger, you should press enroll button. After pressing enroll button, it will ask you to select your fingerprint id number. After the selection of the id number. You have to place your finger. Place your finger and the fingerprint module R307 will register you with the fingerprint id. The fingerprint is stored. You are now ready to vote.

You should be now pressing the fingerprint match key to cast your vote. The voter will place his finger with which he had registered before. If the voter is an authorized voter it will display, he is an authorized voter. The EVM machine will now enable the voter to cast his vote. EVM has a result button that will make us know about the results. As the above, the casting of votes is equal to all its tie.

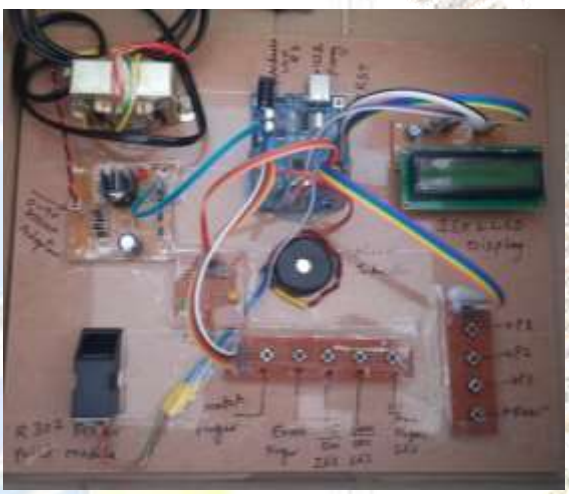

Fig.6: Output of the project work carried

V. CONCLUSION

Ensuring that the election is conducted honestly and without fraud. The system which we have referred to has implemented the authentication electronic voting machine (AVM) in different ways. The most flexible way of implementation is by using the biometric system. Although technology is evolving, the government continues to use outdated EVM machines. The older EVM machines are exceedingly challenging to operate.

We have created a mechanism that will update how the EVM functions. As everyone knows, a person's fingerprint serves as their unique identification. That will vary depending on the individual. Thus, using a fingerprint as a unique identification is preferable. The system stores a fingerprint database of every voter. If a person wishes to cast a ballot for any party, their identity must be verified through a fingerprint-matching method. With a successful fingerprint match, the voter may cast their ballot for any one party. Data analysis is possible in the form of statistics showing the proportion of votes cast for each party. Only a registered voter may cast a vote, and the system alerts users to any fraud. In evaluating the equipment, we obtained precise results.

VI. FUTURE SCOPE

Retinal scanning is also a possibility. Audio output can be added to make it more user-friendly for illiterate voters. The fingerprint device's memory may be increased. External memory can be used to save the fingerprint image, which can then be retrieved for comparison. A smart card reader module is expected to be added to the current module for added security and to minimize database storage. To increase the capacity, we can employ a 1 MB flash drive biometric module.

VII. REFERENCE

[1] Suraj H P, Skanda G, Shobith G Bharamshetty, Srikanth P S, "IoT Based Remote Electronic Voting System Using Aadhar and Dual Biometric Authentication," Iosr Journal of Computer Engineering (Iosr-Jce), E-Issn: 2278-0661, P-Issn: 2278-8727, Vol 17, Issue 4, Ver. Iii (July – Aug. 2020), Pp. 01-10. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Nithya, M.Rohith, K.Nikitha, K.Brugu Sai, L.Pradeep, Y.Prathyusha, Dr. R. Shankar," Fingerprint Based Electronic Voting Machine Using Arduino,". Journal Of Engineering Sciences. Vol 13 Issue 07, July/2022, Issn:0377-9254, Pp. 01-09.

[3] Miral Desai, Hiren Mewada, Jigenesh Patoliya,“ Internet of Things (IoT)-Based Advanced Voting Machine System Enhanced Using Low-Cost IoT Embedded Device and Cloud Platform," *Information and Communication Technology for Intelligent System. DOI: 10.1007/978-981-15-7062-9_8, pp.01-11.*

[4] Abeesh A I, Amal Prakash P, Arun R Pillai, Ashams H S, Dhanya M, Seena R, " Electronic Voting Machine Authentication Using Biometric Information", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, NCETET - 2022 Conference Proceedings.M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[5] Shilpa C Venugopal, Resmi K. Rajan" IOT BASED VOTING MACHINE WITH FINGERPRINT VERIFICATION," International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 1, 2020.

[6] Mr.Sharathchandra N R, Dr. Jose Alex Mathew, Dr. B C Prem Kumar, “IOT Based Fingerprint Voting System,” International Journal Of Engineering Research & Technology, Volume 10, Issue 8 August 2022, ISSN: 2320-2882, Pp. 1-5.

[7] Mr.Sharathchandra N R, Dr. Jose Alex Mathew, Dr. B C Prem Kumar, “IOT Based Fingerprint Voting System,” International Journal Of Engineering Research & Technology, Volume 10, Issue 8 August 2022, ISSN: 2320-2882, Pp. 1-5.

[8] Arun Kumar S, Logesh D, Mageshwaran B, Kavitha Balamurugan, “Iot Based EVM," International Research Journal of Engineering and Technology (IRJET), E-ISSN: 2395-0056, P-ISSN: 2395-0072 Volume: 07 Issue: 04, Apr 2020, Pp. 01-04.

[9] N. Purushotham, B. C. Gopi, R. Kiran Kumar, B. Manasa, K. Balakrishna, "Fingerprint Based Voting Machine Using Iot," Journal of Emerging Technologies and Innovative Research, March 2021, Volume 6, Issue 3, Pp. 1-14, 2019.

[10] Er.Mausmi Dagwar, Chaitali Kawadkar, Saurabh Nidhan, Niraj A. Kurhade, Krunal G. Padole,“Secured Fingerprint Based Voting System Using Iot”, International Journal Of Advance Research And Innovative Ideas In Education, IJARIIE-ISSN(O)-2395-4396, Vol-8 Issue-2 2022.

[11] Vinayachandra, “Arduino Based Authenticated Voting Machine (AVM) Using RFID And Fingerprint for The Student Elections” Et Al 2020 J. Phys.: Conf. Ser. 1712 012004.

[12] Cxotoday.Com,' Internet of Things ' 2023 [Online]. Available: https://www.cxotoday.com/cxobytes/theexpanding-internet-of-things-iot-creates-more-opportunities-for-cybercrime/ [Accessed: 21-03-2023].

[13] Rajguru.Com,' R307 FINGERPRINT MODULE ' 2023 [Online].Available: https://www.rajguruelectronics.com/product/1276/r307%20fingerprint%20module.pdf [Accessed: 21-03-2023].

[14] www.elprocus.com, “Adriano and Rfid”, 2023[ONLINE] Available: https://www.elprocus.com/lcd-16x2-pin-configuration-and-its-working [Accessed: 21-03-2023].

[15] Megalingam, R. K., Rudravaram, G., Devisetty, V. K., Asandi, D., Kotaprolu, S. S., & Gedela, V. V. (2022). Voter ID Card and Fingerprint-Based E-voting System. In Inventive Computation and Information Technologies (pp. 89-105). Springer, Singapore.

[16] Umar, H. S. I., Atte, J., & Haruna, S. (2022). ELECTRONIC VOTING AS AN INSTRUMENT FOR FREE, FAIR AND CREDIBLE ELECTIONS IN NIGERIAN POLITICAL SYSTEM: ISSUES AND CHALLENGES. European Journal of Political Science Studies, 5(2).

[17] Shankar, A., Pandiaraja, P., Sumathi, K., Stephan, T., & Sharma, P. (2021). Privacy-preserving E-voting cloud system based on ID-based encryption. Peer-to-Peer Networking and Applications, 14(4), 2399-2409.

[18] Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021). On the design and implementation of a blockchain-enabled e-voting application within iot-oriented smart cities. IEEE Access, 9, 34165-34176.

[19] Rajesh, G. (2021). Smart Electronic Voting Machine Using IoT. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 1547-1550.

[20] Dagwar, E. M., Kawadkar, C., Nidhan, S., Kurhade, N. A., & Padole, K. G. FINGERPRINT BASED SECURED VOTING SYSTEM USING IOT.