International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 07 | July 2022 www.irjet.net p-ISSN: 2395-0072

SECURED EVM USING BIOMETRIC WITH UNIQUE ID AND IoT

Manjunatha Reddy H S[1], Abhijith G R[2], Adhokshaja N R[3], Ajay Chinnaswamy[4], Aravinda Kumar R V[5]

[1]HOD, Department of ECE, Global Academy of Technology, Bangalore, India
[2345]Student, ECE, Global Academy of Technology, Bangalore, India

---

Abstract - *Elections are important in our democratic society because they let the people decide who will lead their government. In a democracy like India, voting is an essential way for residents to exercise their right to vote. Voters frequently use polling places to cast their ballots. Electronic voting machines are being used to cast ballots more frequently as technology develops. This study proposes a novel methodology with a very secure mechanism. IoT, biometrics, and Aadhar make up its main parts. With biometric fingerprint and face recognition for security and IOT for accurate results, Aadhar ID is a unique card for each individual. The proposed system features secure voting, automatic vote counting, and a highly secure data handling technique.*

Key Words: **Face recognition, fingerprint recognition, EVM, LBPH, Aadhar ID, IoT, Haarcascade.**

1. INTRODUCTION

India has a parliamentary system with a division of power between the federal government and the states, as per its constitution. Elections in this country have a big impact on how the government is run. A candidate for president is chosen using this procedure. The Constitution's requirements led to the creation of India's federal agency, the Election Commission, which is in charge of supervising and managing all elections in the nation. This agency is in responsibility of making sure that elections are free, fair, and unbiased. There are 5 types of elections conducted in India

1. Members of the Parliament in Lok Sabha and Rajya Sabha
2. Members of State Legislative Assemblies
3. Members of State Legislative Councils
4. Members of local governance bodies
5. By-election is held when a seat-holder of a particular constituent dies, resigns, or is disqualified.

This paper examines safe voting practises and how biometrics could enhance elections. The accuracy of the electronic voting system's results has earned the trust of the public because picking a candidate for office is important. As a result, the EVM needs to be built with the utmost security and safety. Voting systems, ballots, punch cards, electronic voting, blockchain—there are many technologies. Network security, microcontrollers, GSM modules, and i-voting are all utilised. However, there are still many issues with EVM in use today. So this study describes a biometric face and fingerprint recognition protected EVM technology employing a special card with IoT. Voters cannot repeat their votes since biometric face and fingerprint recognition are important for identifying individuals. Aadhar is the unique ID number for everyone.

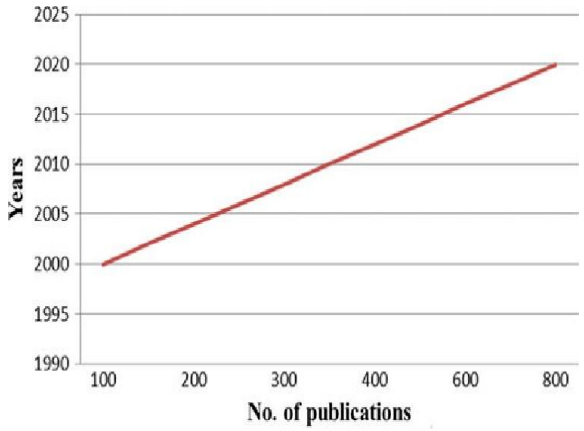

Fig -1: Data for using EVM past 20 years.

Data for using the technology in EVM from the last 20 years in the research community were increasing as shown in Fig.1.

2. LITERATURE SURVEY

[1] S. Kumar, S. Singh, J. Kumar, Live detection of face using machine learning with the multi-feature method. Face identification and detection are crucial areas of study in digital image processing (DIP). These algorithms employ two basic strategies: holistic feature recognition, in which the image data is evaluated as a whole without isolating various parts of a face, and local feature detection based on the geometric model of the human face. Finding human faces independent of their pose, orientation, or imaging situation is the main issue in feature-based facial detection.

[2] B. Shahzad, J. Crowcroft, Trustworthy electronic voting using adjusted blockchain technology. People must maintain their confidence in the vote and the voting process because public faith in democracies is rising. The voting system originated as a means of assisting citizens in electing their representatives, who subsequently form the governments, as a result of growing confidence in democratic institutions. The fundamental functionality of this system is to enable electronic voting, which necessitates aspects like privacy, security, anonymity, and verifiability. To address these problems, the underlying technology must be chosen carefully. It has been determined that Blockchain technology effectively addresses each of these issues. Blockchain technology corrected flaws in the way elections are conducted now by making the voting process transparent and easy to use, preventing fraudulent voting, bolstering data protection, and verifying the results of the election.

[3] R. Rezwan, A. Rahman, Biometrically secured electronic voting machine. In this project, a new voting system based on an electronic voting machine is proposed in light of the drawbacks of the prior voting system (EVM). The voters' fingerprints will be used to provide biometric security, which is another element of this system. Voting systems should be simple to authenticate and verify, have a high accuracy rate, and be very reliable. Additionally, the system must be original and cost-effective. An enhanced voting mechanism is created that makes use of an Aadhaar card, although it is complicated and online. The online method is never completely risk-free. According to this material, the suggested approach will use a fingerprint scanner to identify each voter based on their fingerprint. It can detect if someone is a registered voter or not and it will deny if someone tries to cast a second vote.

[4] Himanshu, G.N. Pandey, Online voting system for India based on AADHAAR ID. This paper makes the first proposal for an online voting system for the elections in India. The suggested methodology offers higher security because the voter's high-security password is verified before the vote is recorded in the Election Commission of India's primary database. The model's added feature allows the voter to verify that the right candidate or party received their vote. In this system, a voter has the option to cast a ballot from a place other than the one designated for them or from their favourite site. The counting of the votes will be done automatically under the proposed approach, saving a significant amount of time and allowing the Election Commissioner of India to declare the results quickly.

[5] S. Anandaraj, R. Anish, P.V. Devakumar, Secured electronic voting machine using biometric. The project suggests and puts into practise a quick and secure technique for collecting votes using biometrics. Technology has changed so much, and as a result, voting has seen several developments. The improvisations reduce the amount of time needed to announce the outcome while boosting the model's flexibility, security, dependability, and scalability. The government database already contained the fingerprint module. Therefore, our initiative offers the greatest way to prevent fraudulent votes. The computer was connected to the electronic voting machine. The computer has a complete database list of everyone who is eligible to vote. The corresponding person's identify was removed for each poll. False voting is therefore prevented. There is a touch screen, so it is user-friendly. A printer is also used to provide a confirmation sheet for the voter who polls the authenticated vote.

[6] Srikrishna Swetha, S. Kumar, A study on smart electronics voting machine using face recognition and Aadhar verification with IoT. It is an electronic voting machine even though the voting machine is a mechanical device that is most frequently created by an electronic material. A very secure voting procedure using face recognition technology is proposed. It was created with a variety of goals in mind, including long-term use, security needs, high voting efficiency and accuracy, among many more. The majority of voters might find this to be useful. Another name for this electronic device is e-voting. It also covers the use of some of the other network kinds, including private computer network use and mobile phone usage.

[7] R.P. Jacobi, F. Trindade, J.P.A. deCarvalho, R. Cantanhede, JPEG decoding in an electronic voting machine, in IEEE 13th Symposium on Integrated Circuits and Systems Design (2000).The Joint Photograph Experts Group established JPEG as a standard for image compression [4, IO]. Due to its lossy nature, which causes data to be wasted during the compression and decompression processes, JPEG performs better with natural photos. The lack of visual information is partially made up for in natural imagery. the visual content. Image information is not lost when using other JPEG formats. The EVM uses the lossy JPEG standard, where the amount of information lost is determined by the compression factor. Images with high compression ratios are subpar. Almost flawless photos are produced by small compress ratios, but little memory is saved.

[8] S. Lavanya, Trusted secure electronic voting machine. In this paper, a secure study of electronic voting machines is analyzed. The electronic device is susceptible to some major threats, according to an analysis. For instance, malicious code on a machine may steal votes covertly if an attacker gained physical access to it or its removable memory card for even a little period of time. Additionally, during regular election activities, a hacker could produce harmful code that spreads silently and automatically from machine to machine. With little to no chance of detection, malicious software operating on a single voting machine can steal votes. This electronic device is capable of figuring out the theft attack. Whoever has direct access to a voting machine or a memory card that will afterwards be loaded

into a machine. In practice, poll workers and others often have unsupervised access to the machines.

[9] M. Karim, S. Khan, An electronic voting system with biometrics is being proposed. The Bangladesh Election Commission (EC) still conducts elections using a manual system in this contemporary era of technology. In this work, we have created an automated biometric voting system with a user-friendly interface and a built-in database system that contains data on every voter. At the conclusion of the voting process, votes will automatically be counted, and the outcome will be generated centrally more quickly. As a result, the suggested system will enhance the management of Bangladesh's elections by ending fraud and corruption, assuring security, openness, fairness, and correctness, and maintaining backup voting process records.

3. PROBLEM DEFINITION

The literature review revealed some significant technical issues with the voting procedure. The voting procedure cannot be accurately and securely counted by hand.

The voting process suffers greatly when votes are missed. In the 2019 elections in India, approximately 21 billion individuals did not cast a ballot, and only a select few had the opportunity to cast two votes in some locations. This occurred as a result of incorrect voter information being registered and a lack of valid identification. Out of the 3,16,671 entries in the voters list, the Election Commission was only able to detect 38,586 double entries, it has been reported to the Kerala high court. One of the main issues with the Indian electoral process is plural voting.

4. OBJECTIVES

• The primary goals of this initiative are to eliminate manual vote counting, stop votes from going uncounted, and stop voters from using multiple ballots.

• Ensuring that a voter is verified in detail before casting a ballot.

• Prevent unauthorized access to the voting process.

• The entire voting process should be digitalized to reduce corruption.

5. DESIGN AND IMPLEMENTATION

The two steps of the suggested approach are the registration of voter information and the voting procedure, as depicted in Fig. 4. The Raspberry Pi3B+, a visual desktop-sharing system of PI, along with a fingerprint reader, webcam, voting buttons, a display, and a connecting cable, make up the hardware components. Python version 3.5 and (SSH) Secure shell were the software components employed. We presented a novel methodology for voting registration, biometric voting, counting issues, and result declaration based on the literature review mentioned above. In the proposed methodology, a webcam with good quality is used to build a real-time face detector and achieve better accuracy. Monitor/screen is used for entering Aadhar numbers, face recognition, and identifying the authorized & unauthorized voters with automatic counting of votes. We have used the LBPH algorithm for the training of images and testing of images. The hardware consists of monitor, voting buttons, connecting cable and wires, and a webcam. VNC viewer works by connecting to the server with an IP address using a username and password.

FACE REGISTRATION

Algorithm (Fig.2)

Step1 Enter ID number

Step2 Capturing images of the face

Step3 Captured successfully

Step4 Images are stored with IDs in haarcascade path.

Step5 Successfully trained

Step6 Registration completed

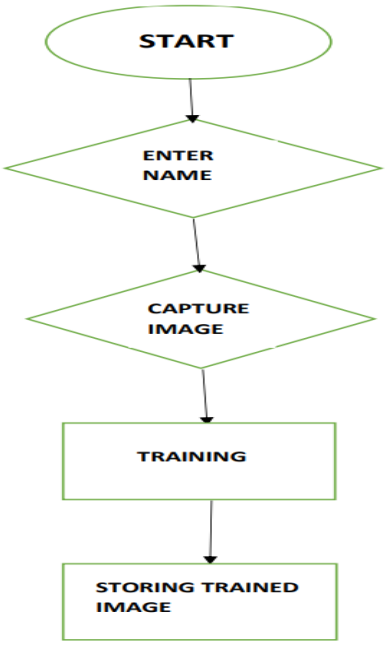

Fig -2: Face registration flowchart.

FINGERPRINT REGISTRATION

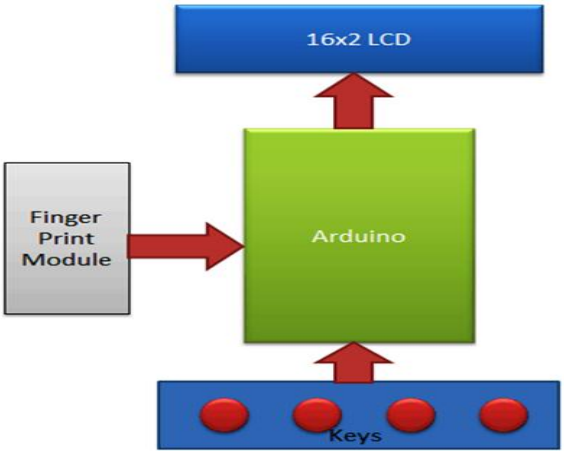

Fig -3: Fingerprint registration.

In our project, we've employed a Fingerprint Sensor Module (R307) to collect thumb- or fingerprint impressions for system input. In this case, the enrol/back, delete/OK, up, and down buttons are all push buttons. There are two features on every key. New finger imprints are entered into the system and the back function using the enrol key. To enrol a fresh finger, the user must first press the enrol key. The LCD will then ask for the ID or location where the user want to store the fingerprint output. The user can now press the enrol key once more to turn around if they decide they do not want to move on at this moment (this time enrol key behave as the Back key).This means enroll key has both enrollment and back functions. DEL/OK key also has the same double function when a user enrolls a new finger then he/she need to select finger ID or Location by using another two key namely UP/MATCH AND DOWN/MATCH (which also has a double function) now user needs to press DEL/OK key (this time this key behaves like OK) to proceed with selected ID or Location. UP/DOWN keys also support the Fingerprint match function.

Working

With the use of a push button or key, the user must enrol a finger. The user must first press the ENROLL key before the LCD prompts them to enter the location and ID where the finger will be saved. Thus, using the UP/DOWN keys, the user must now enter the ID (Location). After choosing Location/ID, the user must press the OK key (DEL key). The LCD will now prompt you to place your finger over the fingerprint reader. The user must now place his finger on the fingerprint reader. The LCD will prompt you to take your finger out of the fingerprint module before asking you to put it back in. The user must now place his finger over the fingerprint reader once more.Now user needs to put his finger again over the fingerprint module. Now fingerprint module takes an image and converts it into templates and stores it by selected ID into the fingerprint module's memory.

VOTING PROCESS

Algorithm (Fig.4)

First, enter your Aadhar number.

Step 2: Showing whether anything is approved or not.

Step 3: If permitted, open the webcam right away.

Step 4: Live face capture and recognition.

Step 5: Display approved or unauthorized using live data and trained images.

Step 6: If the voter is approved, the fingerprint recognition process will begin; else, the vote will not be counted.

Step 7: If permitted, voting is completed after choosing a button.

Step 8: Results display.

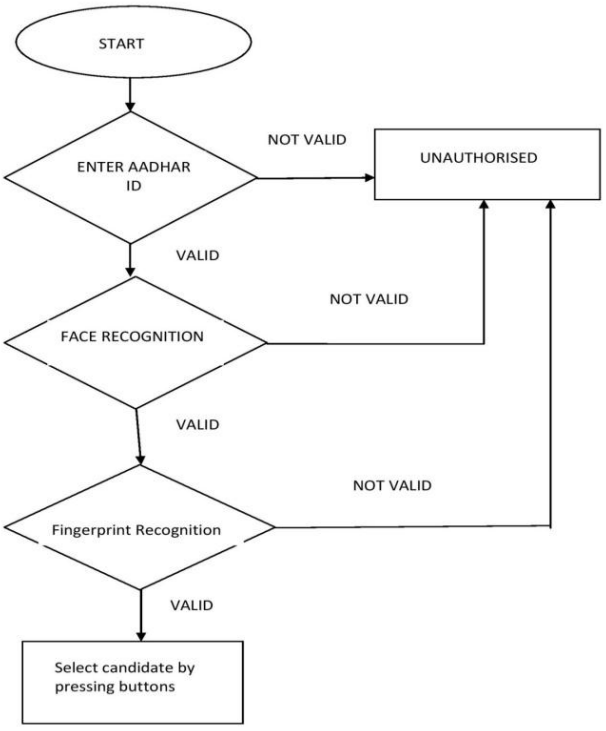

Fig -4: Voting process flowchart.

6. RESULTS

Fig -5: LCD results.

The above figure Fig.5 shows that the voting process is started, by displaying on the LCD as "VOTING MACHINE BY FINGERPRINT".

Fig -6: LCD results.

The above figure Fig.6 explains that a voter is an "AUTHORIZED PERSON" to cast a vote. A person has considered an authorized voter only if his Aadhar id is valid, his face is recognized and his fingerprint is matched.

The below figure Fig.7 explains that a voter to "PLACE A VOTE". This is displayed after face recognition and fingerprint recognition are valid. We have added three different parties Party1, Party2, and Party3. A voter can place a vote by pressing the pushbuttons.

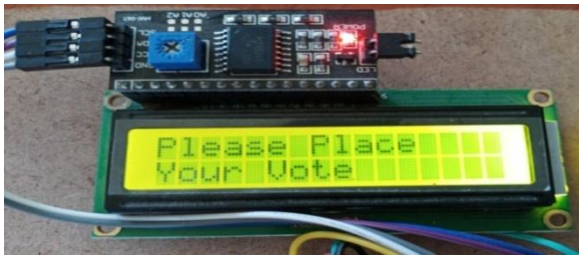

Fig -7: LCD results.

Fig.8 shows the final result in LCD as "VOTE SUBMITTED" after a voter cast his vote for any one of the parties.

Fig -8: LCD results.

Fig.9 shows that a voter's face is recognized and he is an authorized person to vote.

Fig -9: Authorized face.

7. CONCLUSION

Elections in our nation are still not conducted in a very secure manner to ensure fair voting. This suggested approach can include face recognition, better registration procedures, automatic vote counting, storage and transmission of results, and result declaration. Therefore, by doing this, we can prevent double voting, inaccurate registration, and fake biometrics for better elections and a better nation.

REFERENCES

[1] S. Kumar, S. Singh, J. Kumar, "Live detection of face using machine learning with multi-feature method", in Wireless Personal Communication Springer Journal (SCI) Published https://doi.org/10.1007/s11277-018-5913-0

[2] B. Shahzad, J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology". IEEE Access **7**, 24477–24488 (2019).

[3] R. Rezwan, A. Rahman, "Biometrically secured electronic voting machine", in IEEE Region 10Humanitarian Technology Conference (2017).

[4] Himanshu, G.N. Pandey, "Online voting system for India based on AADHAAR ID", in 11th International Conference on ICT and Knowledge Engineering (ICT&KE) (2013).

[5] S. Anandaraj, R. Anish, P.V. Devakumar, "Secured electronic voting machine using biometric", in IEEE International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) (2015).

[6] K. Srikrishna Swetha, S. Kumar, "A study on smart electronics voting machine using face recognition and Aadhar verification with IoT", in 7th International Conference on Innovations in Electronics & Communication Engineering (ICIECE—2018), vol. 65,(Springer, 2018).

[7] R.P. Jacobi, F. Trindade, J.P.A. de Carvalho, R. Cantanhede, "JPEG decoding in an electronic voting machine", in IEEE 13th Symposium on Integrated Circuits and Systems Design (2000).

[8] S. Lavanya, "Trusted secure electronic voting machine", in International Conference on Nanoscience, Engineering, and Technology (2011).

[9] D. Karima, Pr. T. Victor, Dr. R. Faycal. "An improved electronic voting machine using a microcontroller and a smart card", in 9th International Design and Test Symposium (IEEE, 2014).