IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 13, Issue 4, April 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.317

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 4, April 2024||

| DOI:10.15662/IJAREEIE.2024.1304057 |

Voter Recognisation by Face or Finger Print Using Advanced IDE

Rekha Kulkarni, M. Nanda Kumar, G.M. Rohith Reddy, A.Naveen, E.S.Pruthviraj, N.Eshwar

Asst. Professor, Department of ECE, Kuppam Engineering College, Kuppam, Andhra Pradesh, India

B. Tech Final year, Department of ECE, Kuppam Engineering College, Kuppam, Andhra Pradesh, India

B. Tech Final year, Department of ECE, Kuppam Engineering College, Kuppam, Andhra Pradesh, India

B. Tech Final year, Department of ECE, Kuppam Engineering College, Kuppam, Andhra Pradesh, India

B. Tech Final year, Department of ECE, Kuppam Engineering College, Kuppam, Andhra Pradesh, India

ABSTRACT: The Smart Voting System outlined in this project leverages IOT-enabled embedded devices and Python programming to enhance the efficiency and security of traditional voting procedures. By integrating microcontrollers, biometric or smart card readers, push or touch screens and IOT, the system creates a connected infrastructure for seamless interactions between voters and a central server. Python, in conjunction with Flask or Django, is employed for server-side for managing voter authentication, real-time monitoring, and secure storage of voting data in databases. The provided code snippet offers a foundational structure, ensuring one vote per eligible voter and emphasizing the importance of compliance with local regulations and security standards to establish a reliable and trustworthy Smart Voting System.The proposed Voting System that allows the voters to scan their face afterwards scan their fingerprint, which is then matched with an already saved data within a database that is retrieved from Aadhaar card database of the government. Moreover identifying the true identity of the voter is more concerned in our project.

KEYWORDS: IOT, Python, Microcontrolle, CorticalDjango,Flask,voting system

I. INTRODUCTION

Voter authentication is a critical component of ensuring the integrity and security of elections. The development of secure and accurate Voting system with advanced technologies is a crucial and important for building a better democracy.

Voter registration is one of the most important activities that an electoral management body(EMB) or Election Commission of India(ECI) needs to conduct, but it is also one of the costliest in terms of both time and resources. A credible voter register confers legitimacy on the electoral process, helps prevent electoral fraud and ensures that every eligible voter can vote in an election and that they can do so only once.An inaccurate voter register can cause problems in the electoral process by raising doubts about the election'sinclusiveness and outcome and by opening up avenues for fraud and manipulation.

Many countries that face challenges in creating an accurate voter register are considering reforming their voter registration systems through the introduction of biometric and face recognition technologies.

In traditional Voting System, each voter has to carry an identity proof which is used to establish the identity of the person. The identification process takes a lot of time since every person has to prove his identity individually and then only,he or she is allowed to cast the vote.Also,voting is a very sensitive process because the chances of forgery are high. In order to simplify the process and avoid various errors, we have developed face recognition voting machine which uses a person's face id as the proof of his identity as all the data is available with National Informatics Centre (NIC) and Unique Identification Authority of India (UIDAI)i.e. Aadhaar. There will be no need for the person to carry documents regarding his identity.

Biometrics is the science and technology of measuring and analyzing biological data. Biometrics refers to technologies that measure and analyzes human body characteristics, such as DNA, fingerprints, eye retinas and irises,

Fig 1: Manual/In-personverificationof voter.

The field of biometrics was formed and has since expanded on too many types of physical identification. Among the several human fingerprints remain very common identifier and the biometric method of choice among law enforcement. These concepts of human identification have led to the development of fingerprint scanners that serve to quickly identify individuals and assign access privileges. The basic point of these devices is also to examine the finger print data of an individual and compare it to a database of other fingerprints.

Face recognition technology has the potential to provide a more secure andreliablemethodofverifyingtheidentityof voters. By analyzingandcomparingunique facial features, such as the distance between the eyes or the shape of the nose, face recognition systems can accurately identify individuals with a high degree of accuracy.

II. OBJECTIVE

In this project report, we explore the use of biometric and face recognition technology for voter authentication using a RaspberryPi. The RaspberryPi isaversatile and affordable single-board computer that can be easily integrated into a variety of applications. Biometric data to ensure secure and accurate voter verification.

LeveragingthecapabilitiesofRaspberryPi,mini-computer, this systemoffersareliable and efficient way to authenticate voters.
Hencewiththeapplicationofthisfingerprintandfacerecognition-basedVoting system, elections could be made fair and free from rigging. This innovative approach notonlyenhancesthesecurityofthevotingprocessbutalsostreamlinestheverification process for a seamless voting experience

➢ The primary objective of integrating face and biometric recognition into the Smart Voting System is to enhance voter authentication, thereby ensuring the integrity and security of the electoral process.

➢ By leveraging IoT-enabled embedded devices and Python programming, the system aims to streamline the voter identification process while minimizing the risk of fraudulent voting. Through the use of biometric or smart card readers, the system will verify the identity of each voter, allowing only eligible individuals to cast their votes.

➢ This objective seeks to improve the efficiency and reliability of the voting procedure while adhering to local regulations and security standards, ultimately fostering trust in the electoral system.

Ultimate objective is to identify the true identity of the voter.

III. METHODOLOGY

The use of biometric and facial recognition for authenticating the voter with raspberry pi follows the following methodology.
SystemArchitectureDesign: Definetheoverallarchitectureofthesystem,including hardware component (Raspberry Pi, camera module, fingerprint module, buzzer, lcd module, push buttons) and software modules (facial and biometric recognition algorithm, database integration, user interface).

Biometric Data Acquisition: Select appropriate biometric modalities (e.g., facial recognition, fingerprint scanning)forvoter authentication. Integrate biometricsensors with the Raspberry Pi platform to capture biometric data from voters securely and efficiently.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 4, April 2024||

| DOI:10.15662/IJAREEIE.2024.1304057 |

Biometric Template Extraction: Develop algorithms to extract unique biometric templates from the acquire data, such as facial features or fingerprint patterns. Implement feature extraction techniques to convert biometric data into a standardized format suitable for comparison and matching.

Template Enrollment: Design user-friendly interface forvoter registration, allowing individuals to enroll their biometric data into the system. Store biometric templates securely in a database, associating each template with the corresponding voter's identity.

Authentication Process: Develop algorithms to compare newly captured biometric data with enrolled templates to verify the identity of voters. Implement matching algorithms with thresholding mechanisms to determine the level ofsimilarity required for authentication.

Integration with Facial Recognition: Utilize facial recognition algorithms to extract facial features from captured images or video streams using the Raspberry Pi camera module. Integrate facial recognition with the biometric authentication process to enhance the accuracy and robustness of voter verification.

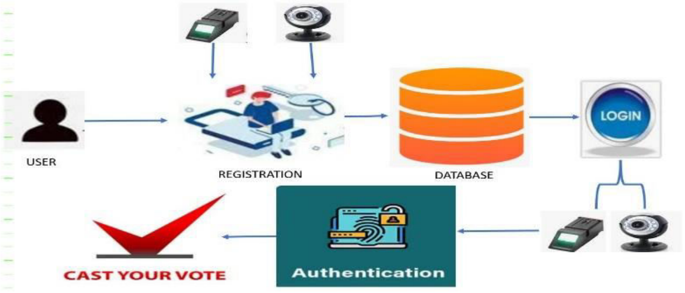


Fig 2: Methodology

Data Collection and Preprocessing: Collect a diverse dataset of facial images from

Feature Extraction: Utilize pre-trained deep learning models (e.g., Convolutional Neural Networks) to extract discriminative features from facial images. Fine-tune the mode life necessary to optimize performance for the specific task of voter authentication**.**

Model Training: Train the facial recognition model using the preprocessed dataset, leveraging techniques such as transfer learning to adapt the model to the voter authentication task. Employ strategies to address biases and ensure fairness in the recognition process.

Database Integration: Establish a secure database to store biometric data and facial embed ing so fregistered voters. Develop mechanisms to efficiently query the database for matching facial and biometric features during the authentication process.

System Implementation: Develop software modules to implement biometric and facial recognition functionalities on the Raspberry Pi platform. Ensure seamless integration between hardware components (biometric sensors, camera module) and software modules.

User Interface Design: Design an intuitive user interface for election officials and voters to interact with the authentication system. Provide clear instructions and feedback to guide users through the authentication process effectively.

Testing and Validation: Conduct thorough testing to evaluate the performance, accuracy,andre liability of the authentication system under various conditions.Usetest scenarios to simulate real-world use cases and identify potential issues or limitations.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 4, April 2024||

| DOI:10.15662/IJAREEIE.2024.1304057 |

Security and Privacy Measures: Implement encryption protocols to secure communication between the Raspberry Pi and the central server/database. Incorporate security measures to protect biometric data from unauthorized access, tampering, or misuse. Ensure compliance with data protection regulations and privacy standards to safeguard voter privacy.

IV. EXISTING SYSTEM

Fig 3: Manual identification of voter:

For projecting of votes with EVMs, the citizens need to deliver their Election Photo Identity Card (EPIC) gave by the Election Commission. The surveying official
Requirements to check the EPIC with the official run down he has, at that poin the needs to affirm if it is an approved card and he permits the citizens to project their votes. In this way EVMs relyon manual check of the EPIC which is consuming more time.

This way EVMs rely on manual check of the EPIC which is consuming more time.

V. PROPOSED SYSTEM

Theproposedsystemisdividedintoseveralblockslikeinput data gathering, preprocessing, training and accessing the data stored in the data base.

- Inordertoovercometheproblemsintheexistingmethod,ourproposedsystem which is highly secured and fraudulent vote detection based smart EVM.
- In this the verification is done by using biometric (finger print) as well as with face i.e. Aadhar based.
- Thevoterhastoscantheirfingerinthebiometricandfacethroughwebcamera, itwillautomaticallyverifythetrueidentityofvoterandenablethevotertocast whenIDismatchedthepersonisvalidtovote.Iffingerprintdoesn'tmatch Itis considered as fraudulent/he has no authority to vote in that election.

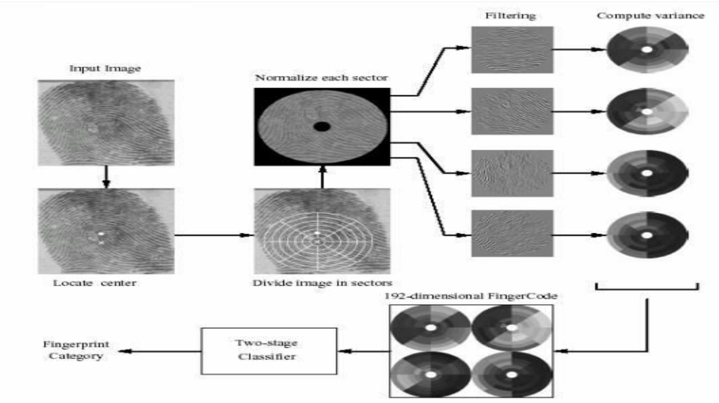


Fig 5: Classification of finger print from input image/fingerprint.

| DOI:10.15662/IJAREEIE.2024.1304057 |

VI. HARDWAREIMPLEMENTATION

Theproposedsystemisdividedintoseveralblockslikeinputdata gathering, preprocessing, training and accessing the data stored in the data base.

Classifying faces with a webcam typically involves using computer vision techniques and machine learning algorithms. Here's a general outline of how this process might work:

1. FaceDetection: The first step is to detect the presence of faces in the webcam feed. This is often done using a technique called Haar cascade classifiers or more advanced methods like deep learning-based face detectors (e.g., using Convolutional Neural Networks - CNNs). Once a face is detected, its bounding box coordinates are usually provided.

2. Face Alignment and Preprocessing: After detecting a face, it's often necessary to alignit properly for further analysis. This involves adjusting the orientation of the face to a standardized pose. Preprocessing steps such as normalization, resizing, and Possibly gray scale conversion might also be applied to improve the quality of the input data

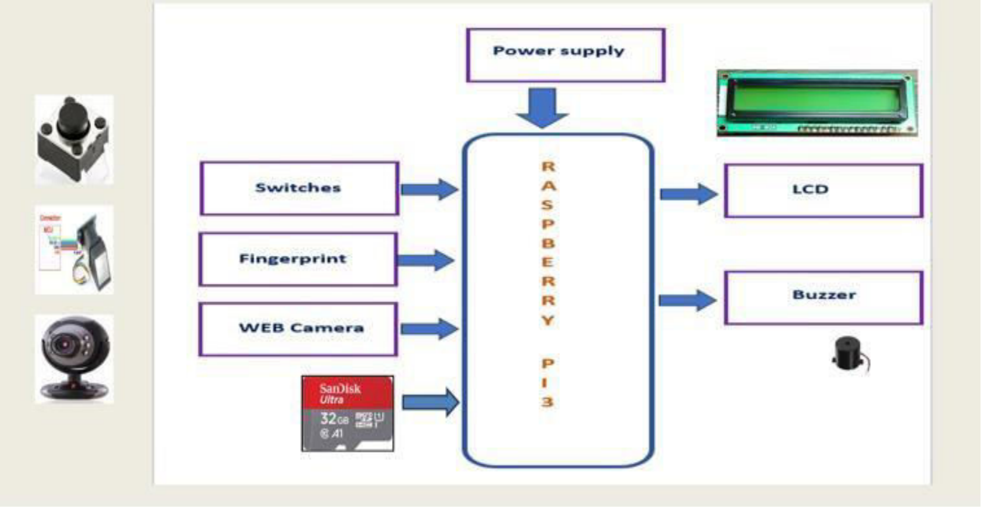


Fig 6.Block Diagram Of System

3. Feature Extraction: Once the face is properly aligned and preprocessed, features are extracted to represent the facial characteristics. These features could include istogram of Oriented Gradients (HOG), Local Binary Patterns (LBP), or deep features extracted from pre-trained CNN models.

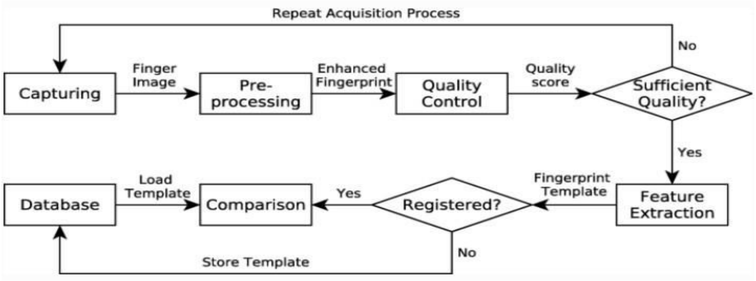
4. Classification: With the extracted features, a classification algorithm is used to categorize or recognize the face. This could be a tradition almachinel earning classifier such as Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), Random Forests, or more advanced techniques like deep learning-based classifiers.

5. Post-processing and Decision Making: Depending on the application, post- processing steps might beapplied to refinethe classification results. Forexample, in a facial recognition system, additional verification steps might be taken to confirm the identity of the detected face, such as comparing it against a database of known faces.

6. Feedback Loop (Optional): In some cases, a feedback loop may be in corporate to improve the classification accuracy over time. This could involve collecting user feedback on the classification results and using it to update and fine-tune the classification model.

Overall, the process of classifying faces with a webcam involves a combination of techniques from computer vision, machine learning, and possibly deep learning,
Tailoredtothespecificrequirementsandconstraintsofthe application.

A. Fingerprint Acquisition Process:



- Finger image or finger photo refers to an image acquired using a touch less capture device, e.g.,smart phone camera, biometric sensor, which contains one or more fingers of a subject.
- Finger print image refers to a finger image cropped to an area representing a finger print, i.e., finger tips.
- Finger print refers to a preprocessed touch less finger print image or a fingerprint captured by a touch-based sensor.

Acquisition: A homogeneously illuminated; noise-free finger image should be acquired. High-quality camera equipment and a predictable illumination are a good precondition for a proper finger image.

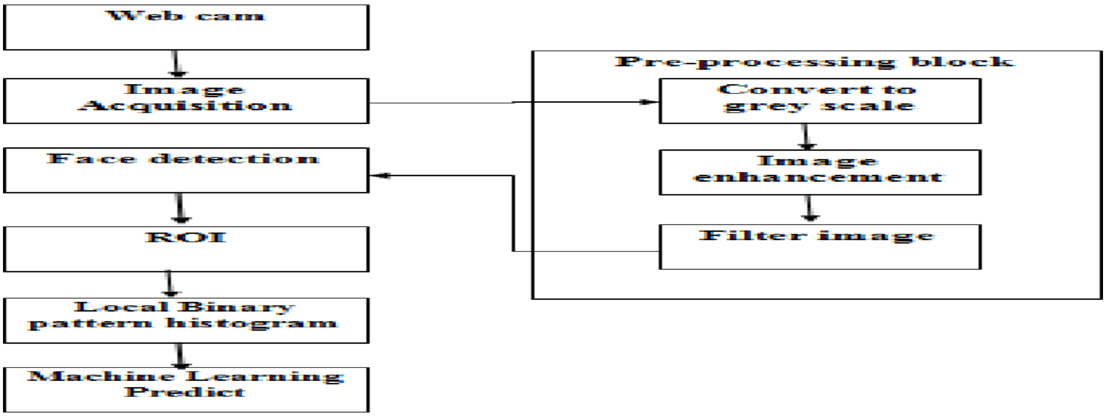
Preprocessing: An accurately segmented and rotated fingerprint images yield meaning ful comparisons cores. At this point, user instructions or a finger print guidance during the capturing process can help to increase accuracy. Quality assessment: A dedicated quality assessment which is integrated in the preprocessing pipeline is crucial to consider only samples of high quality.

Feature extraction and comparison: A specific touch less feature extraction which is adapted to the considered dataset reveals results comparable to touch-based schemes.

Challenges: Uncontrolled background, Varying illumination, Finger position, Impurities on the finger surface.

B. Face ID Acquisition Process:

FaceAcquisition Process



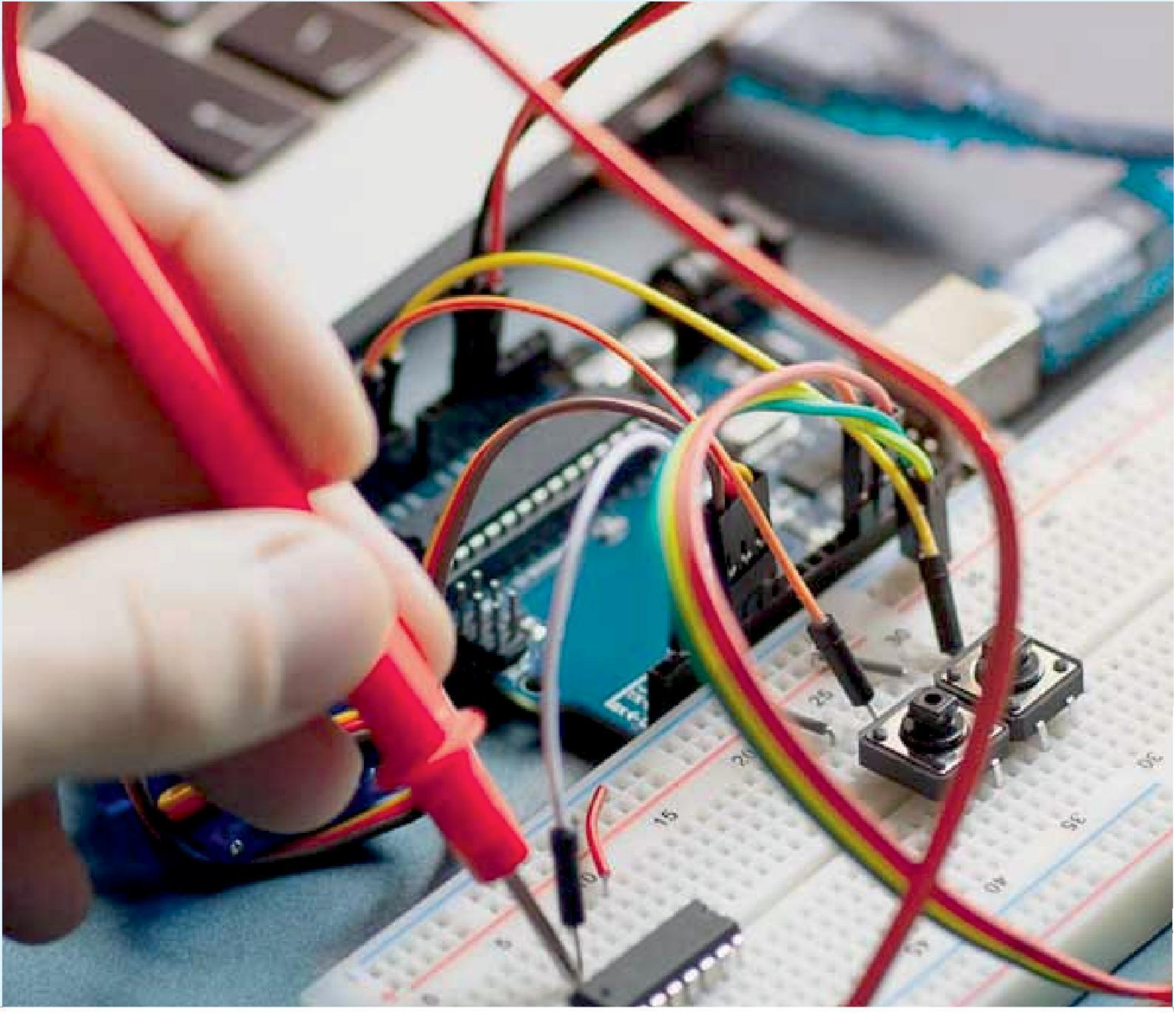
VII. CONCLUSION

The proposed secured Online voting system uses Aadhar card and Voter Id for authentication. Database consisting of the details like name, address, age, gender and fingerprint should be updated every time before election. This system affords additional security by allowing voter to vote only once by comparing unique identification.

The proposed system has end-to-end verifiability which increases the trust of voters on voting system, it is equipped with extra security layer with transparent in voting process, easy to handle and there are no complex tasks required for governing authority as well as which may lead into increase in voting. to reduce the proxy vote and in booth capturing situation this system help us.

REFERENCES

1. Mr. S. Glad win Moses Stephen,"AAADHAR Based Voting System Using Biometric Authentication and IOT", March 2017..
2. Mr. S. Glad win Moses Stephen ,"AADHAR Based Voting System Using Biometric Authentication and IOT ",March 2017, Shubham T. Jadhav, Aadhar Based Electronic Voting System" International Jou.
3. Prof. R. L. Gayle, Vishnu Lokhandernal of Advance Scientific Research and Engineering Trends, May 2016 [4] B. Mary Haque G. M. OwaisAhmed, "Fingerprint and RFID Based Electronic Voting System Linked with Aadhar For Rigging Free Election", International Journal of Advance Research in Electrical, Electronic and Instrumentation Engineering, March 2016.
4. Smita B. Khairnar P. Sanyasi Naidu, ReenaKharat, "Secure Authentication for Online Voting System" International Journal of Computer Science and Information 2015.
5. Sanjay Kumar Premarket Sing, "Design a Secure Electronic Voting System Using Fingerprint Technique", IJCSI International Journal of Computer Science Issues, Vol.10, Issue 4, 2013.
6. https://www.eci.gov.in/evm/
7. https://ieeexplore.ieee.org/document/10073982
8. https://www.ijert.org/research/smart-voting-system-by-using-iot-IJERTV13IS020063.pdf
9. https://www.researchgate.net/publication/3582438_13_Smart_Voting_System_Using_Facial_Recognition
10. https://ijrpr.com/uploads/V4ISSUE8/IJRPR16105.pdf



International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details