IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134218

Secure Vote - Augmenting Democracy with Aadhar linked Biometrics

Adhya Shetty P[1], Anushree[2], Ashwitha[3], Mayoori P[4]

A J Institute of Engineering and Technology, Mangaluru, India[1-4]

Abstract: Elections are the mechanisms through which citizens choose their leaders by casting votes, traditionally using ballot papers or Electronic Voting Machines (EVMs). However, these conventional voting methods are susceptible to misuse and vote rigging. To address these issues, this research proposes a secure voting system that incorporates fingerprint scanning and facial recognition technologies. The proposed system ensures a safe and tamper proof election process by employing fingerprints and facial features as unique biometric identifiers for voter registration and authentication. During the registration process, voter's face are captured, extracted, and securely stored in a database, preventing multiple registrations by the same individual. On the voting day, voters must verify their fingerprints and face, which are then compared against the database. If a match is found, the system authenticates the voter's identity using their Aadhar number, Facial recognition and fingerprint. This approach effectively mitigates the risk of duplicate registrations, leading to a higher rate of successful and legitimate voting.

Keywords: Facial Recognition, Aadhar number, Fingerprint Scanning.

I. INTRODUCTION

The Secure Voting System introduces an advanced and secure approach to the voting process by leveraging Aadhar cards and biometric data, specifically facial recognition and fingerprint scans. This unique identification method serves as a personalized key that only the rightful voter possesses, minimizing the risk of fraudulent voting and ensuring that each vote is cast by its legitimate owner. It establishes a strong connection between a voter's identity and their right to participate in the democratic process, akin to a special lock for each vote, adding an extra layer of fairness and transparency to the electoral process. By combining Aadhar cards with biometric data, the system enhances the reliability of the verification process and instils confidence in the overall integrity of the electoral system. This innovative approach acts as a safeguard, reinforcing the democratic foundation by preventing identity fraud and setting a precedent for secure and transparent electoral practices. The Smart Voting System fosters trust in the democratic system by ensuring that each vote is genuine and accurately attributed to the rightful voter, thereby upholding the principles of fairness and representation in governance. It reinforces the connection between a voter's identity and their right to participate in the democratic process, serving as a personalized key that only the legitimate voter possesses, ultimately enhancing the security and accuracy of elections.

II. MOTIVATION

The current voting system faces significant challenges in preventing voter fraud, instilling public confidence, and ensuring the integrity of the electoral process. Voting can be tricky because sometimes dishonest people try to vote more than once by pretending to be someone else. That's not fair at all! To fix this, we can use Aadhar cards along with fingerprints and face scans. Think of your fingerprints and face like special keys that only you have. This means only you can use them to vote. With this system, we can make sure each person votes just once with their own identity. Checking fingerprints and faces also helps people with disabilities or those who struggle to read. By establishing a robust link between a voter's identity and their right to vote, this system can effectively prevent voter impersonation, duplicate voting, and other forms of electoral malpractice. Overall, this new system with Aadhar and biometrics will make voting more modern, fair, and trustworthy. People will feel more confident that their votes count, and elections will be truly fair for everyone.

III. OBJECTIVES

- Implement advanced biometric features, such as face and fingerprint scans, to strengthen voter identification and authentication.
- Integrate the voting system with the Aadhar database, leveraging its comprehensive and secure repository of citizen information.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134218

- Create a tamper-proof voting system by leveraging Aadhar database for a secure foundation, safeguarding against manipulation and ensuring integrity.
- Simplify voter authentication with Aadhar-linked biometric data for accurate and efficient voting.
- Promote electoral transparency using advanced tech and Aadhar database for a secure, reliable platform, fostering voter trust.

IV. SYSTEM DESIGN

Architectural design is a creative process where you try to establish a system organization that will satisfy the functional and non-functional system requirements. Because it is a creative process the activities within the process differ radically depending on the type of system being developed, the background and experience of the system architect, and the system requirements for the system.

A. Flow Chart

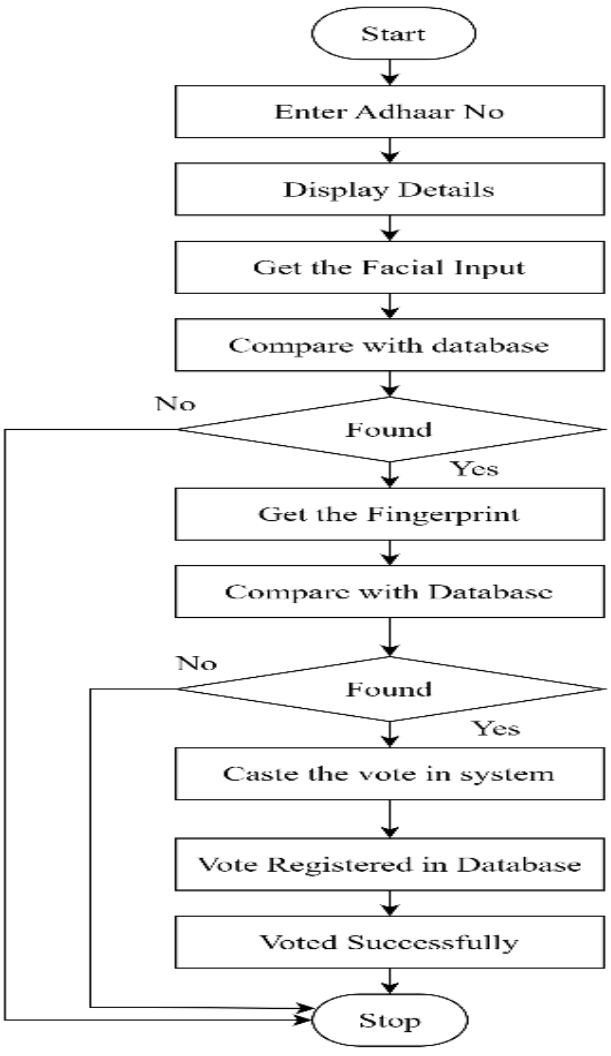

Figure 1 Flow Chart

The voter initiates the process by entering their Aadhaar number, which serves as a unique citizen identification, prompting the system to retrieve and display their personal details from the database. The voter must then provide a facial input captured through a camera, which is compared against their stored facial biometric data from the registration process, if there is no match, the process may terminate or require additional verification steps. Next, the voter provides a fingerprint input via a fingerprint scanner, which is compared against their stored fingerprint biometric data; again, a mismatch may result in termination or extra verification. After successful facial and fingerprint biometric authentication, the voter can proceed to cast their vote electronically. Once the vote is cast, it is recorded and registered in the database

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134218

against the voter's Aadhaar number, and a confirmation message is displayed. The use of Aadhaar numbers and facial/fingerprint biometric authentication to verify the voter's identity before allowing them to vote is a key aspect aimed at ensuring the integrity and security of the voting system by preventing unauthorized access and voter impersonation.

B. Architecture

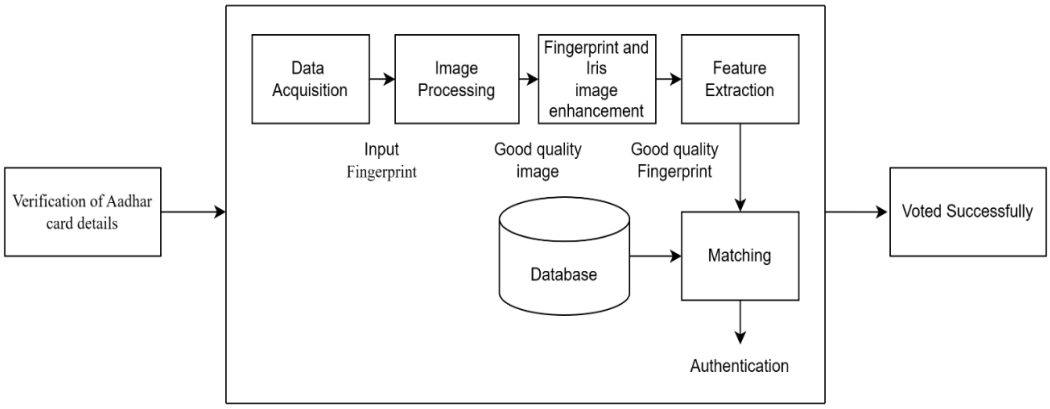

Figure 2 Architecture

The process aims to ensure the integrity and security of the voting system by preventing unauthorized access and voter impersonation. The voting system utilizing facial recognition and fingerprint scanning for identification. Voters representing the participants, Face Detection and Finger Detection indicating the use of facial recognition and fingerprint scanning technologies for identity verification, Aadhar Number linking biometric data to unique identification numbers, and Candidates and Results handling the selection process and outcome of the election. Biometric authentication, particularly through facial recognition and fingerprint scanning, holds the security of voting systems. By requiring individuals to undergo biometric verification, the likelihood of unauthorized voting or fraud can be reduced. These technologies offer unique identifiers that are difficult to replicate, enhancing the integrity of the voting process. Facial recognition analyses distinct facial features, while fingerprint scanning relies on unique patterns, providing a dual-layered approach to authentication.

V. SYSTEM IMPLEMENTATION

A. Algorithm Used

The Local Binary Pattern (LBP) is a method used for person recognition. It starts by converting the image of a person to grayscale, where each pixel has a value between 0 and 255. Then, a 3x3 window or matrix is taken from a portion of this grayscale image. The pixel values in the neighbourhood of the central pixel are compared to the central pixel's value. If a neighbouring pixel's value is greater than the central pixel, it is given a binary value of 1, otherwise 0. These binary values are then converted to a decimal value and assigned to the central pixel. This process continues using a sliding window approach, creating a new image with enhanced characteristics compared to the original.

Face recognition is performed by extracting the histogram from this LBP result image. The image is divided into GRID X and GRID Y blocks, and each region yields a histogram value between 0 and 255 (since it's grayscale). All the regional histograms are then concatenated. If the concatenated histogram of the test image is closer to the trained original image's histogram, the face is recognized. Otherwise, it's not recognized. The Euclidean distance method is commonly used to compare the histograms of the two images and determine face recognition.

B. Dataset

The face database is created by capturing images from a video recorded using a webcam.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134218

Figure 3 Dataset

These facial images of individuals are stored in a folder named "dataset," which serves as the database for face recognition. For each person or subject to be recognized, 101 images are included in the database. Therefore, if there are 10 different individuals, the dataset would consist of a total of 1010 images (101 images per person). The number of images per person in the database remains constant at 101, and the overall size of the dataset expands proportionally to accommodate additional individuals for recognition purposes. This dataset, comprising facial images obtained from video recordings, forms the foundation for the face recognition system to learn and identify individuals effectively.

C. Fingerprint Module

The Fingerprint Module is a serial fingerprint scanner that directly connects to the computer's communication port. It utilizes the MAX232IC to enable seamless connectivity between the R305 Fingerprint Sensor and any controller. This fingerprint scanner has the capability to store and compare fingerprint data, providing the desired output as a result. The core functionality of the system relies on a matching algorithm technique, which compares previously recorded fingerprint templates against users' fingerprints for authentication purposes. Leveraging biometric technology enhances the project's security, and this all-in-one optical fingerprint sensor streamlines the process of fingerprint recognition and verification, offering a convenient and reliable solution.

VI. RESULT ANALYSIS

Figure 4 Home Page

The above figure shows home page of the system, it contains admin and user login option. Admin can register a new voter and do authentication of new voter.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134218

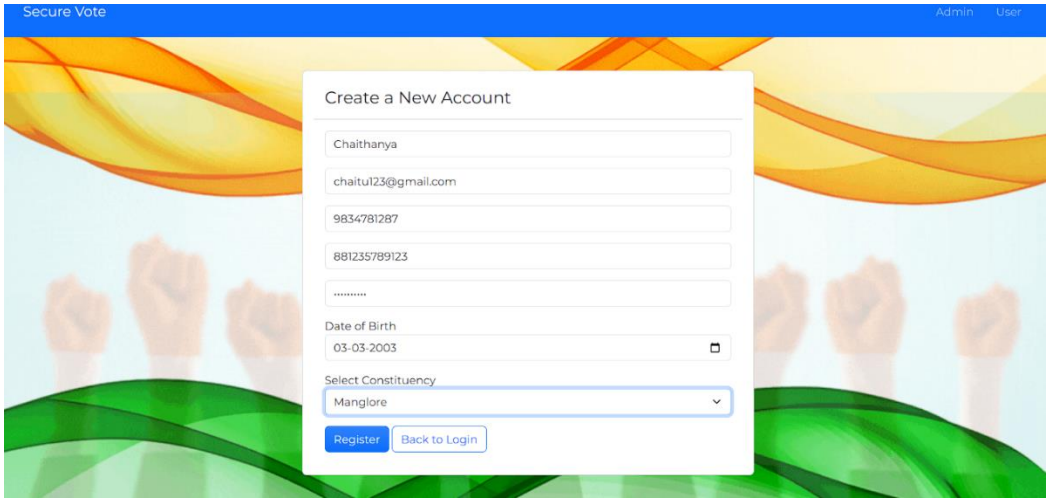

Figure 5 Voter Registration

The above figure shows voter registration page, where new voter can register by using their personal details such as name, email address, phone number, Aadhar number, password, date of birth and constituency.

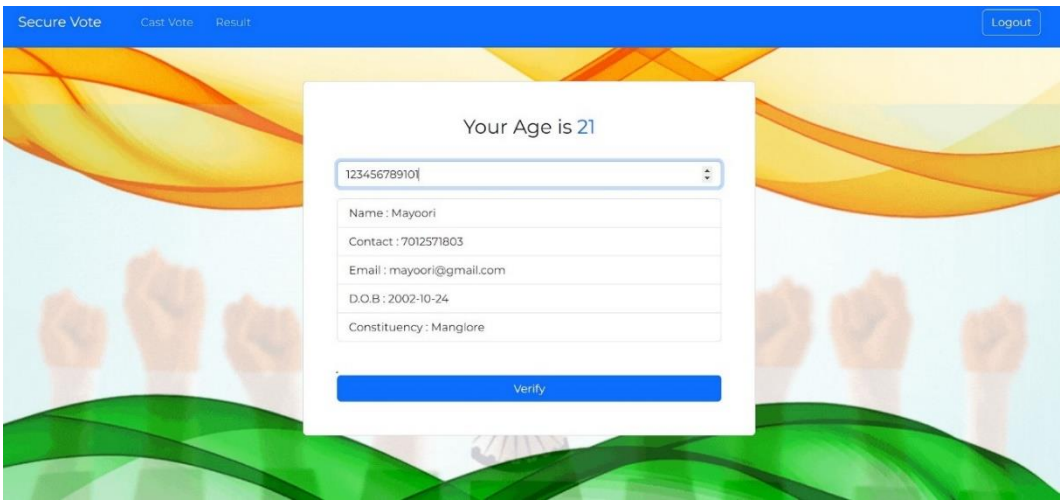

Figure 6 Voter Details

The above figure shows the voter details in user side. When a user caste his vote he has to enter his Aadhar number. After entering Aadhar number the details of the users gets displayed. When you click verify button we have scan our fingerprint then face when successfully verified the casting vote page opens.

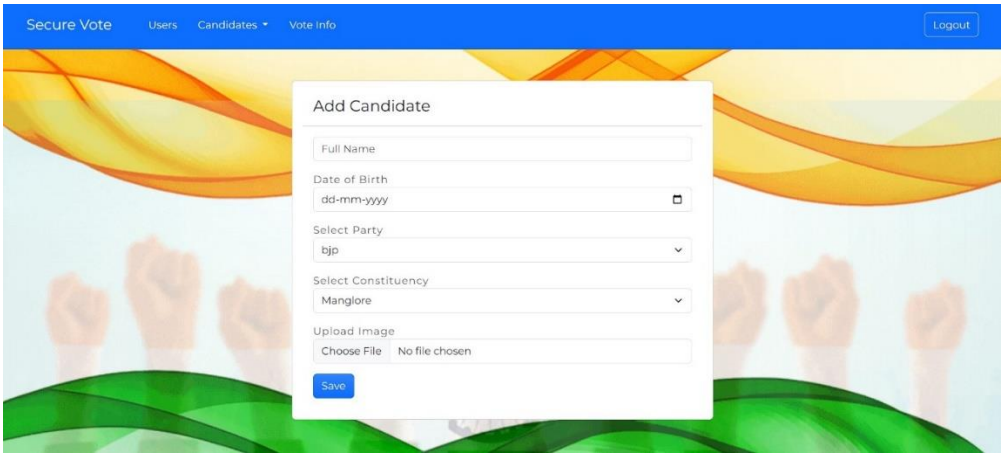

Figure 7 Add Candidate

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134218

The above figure shows adding of candidate to specific Constituency.

```
import cv2
import numpy as np
faceDetect = cv2.CascadeClassifier(r'''haarcascade_frontalface_alt2.xml''');
cam = cv2.VideoCapture(0);

id=input('enter the user id');
sampleNum=0;
while(cv2.waitKey(1)!=27):
    ret,img = cam.read();
    print(img);
    gray = cv2.cvtColor(img,cv2.COLOR_BGR2GRAY)
    faces = faceDetect.detectMultiScale(gray,1.3,5);
    for(x,y,w,h) in faces:
        sampleNum=sampleNum+1;
        cv2.imwrite("dataset/User."+str(id)+"."+str(sampleNum)+".png",gray[y:y+h,x:x+w])
        cv2.rectangle(img,(x,y),(x+w,y+h),(0,0,225),2)
        cv2.waitKey(100);
    cv2.imshow("Face",img);
    cv2.waitKey(1);
    if(sampleNum>100):
        break;
cam.release()
cv2.destroyAllWindows()
```

Figure 8 Code snippet to capture and store image

This code is used to detect and capture image from the webcam using Haarcascade and train it using algorithm and store.

VII. CONCLUSION

The implementation of a voting system using Aadhaar numbers and biometric authentication, including facial and fingerprint recognition, has the potential to revolutionize the electoral process in India. This system aims to address challenges faced by traditional voting methods by integrating cutting-edge technologies such as machine learning, biometrics, and secure data management. It begins with a robust registration module that verifies voter eligibility, collects personal details, Aadhaar numbers, and biometric data, which are securely stored and used to train accurate biometric recognition models through machine learning algorithms. The registration process also associates each voter with their respective constituency, ensuring they can cast their vote for the appropriate candidates. On the voting day, the system employs a multi-factor authentication approach, requiring voters to present their Aadhaar numbers and undergo biometric verification through facial recognition and fingerprint scanning. This two-step biometric authentication process significantly reduces the risk of voter impersonation and multiple voting, thereby enhancing the integrity of the voting process.

REFERENCES

[1] S. Agarwal, A. Haider, A. Jamwal, P. Dev and R. Chandel, "Biometric Based Secured Remote Electronic Voting System," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-5, doi: 10.1109/ICSSS49621.2020.9202212.

[2] P. M. B. Mansingh, T. J. Titus and V. S. S. Devi, "A Secured Biometric Voting System Using RFID Linked with the Aadhar Database," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 1116-1119, doi: 10.1109/ICACCS48705.2020.9074281.

[3] S. J. J. ARPUTHAMONI and A. G. SARAVANAN, "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 1-7, doi: 10.1109/ICICV50876.2021.9388405.

[4] K. Hasta, A. Date, A. Shrivastava, P. Jhade and S. N. Shelke, "Fingerprint Based Secured Voting," 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, 2019, pp. 1-6, doi: 10.1109/ICAC347590.2019.9036777.

[5] BalaMurali; Potru Sarada Sravanthi; B. Rupa, "Smart and Secure Voting Machine using Biometrics" 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-5, doi: 10.1109/ICSSS49621.2020.9202212.