IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 11, Iss 12, 2022

AN INNOVATIVE APPROACH FOR E-VOTING SYSTEM BY MULTIMODAL BIOMETRICS IN INDIA

Amitesh yadu[1]
Research Scholar, School of IT
[1]MATS University, Raipur (CG), India
amiteshyadu1@gmail.com
Dr. Snehlata Barde[2]
Professor, School of IT
[2]MATS University, Raipur (CG), India
drsnehlata@matsuniversity.ac.in

Abstract: - Voting has evolved over the years from a purely manual process to more electronic means. The use of electronic devices in voting is Known as electronic voting. By electronic voting we need to be able to make sure the ballot cast can be authentic must be verified and the transaction cannot be traced Voting process is strictly followed in India The principle of Electronic Voting Machine (EVM) is simple design, reliable and fast access characteristics. Unfortunately, due to hardware problems in EVMs, Faulty officials and illegal voters have illegal votes being cast. This research paper introduced an innovative approach to designing an E-Voting system with the help of multimodal biometrics that enhances security, overcomes the chances of fraud, and provides high-level authentication. High Accuracy is achieved by the fusion of facial and fingerprint recognition Arrangements.

INTRODUCTION

Voting has evolved over the years from a purely manual process more electronic means. Use of electronic devices in voting Known as electronic voting. By electronic voting we need to be able to make sure the ballot cast can be authentic must be verified and the transaction cannot be traced. The current voting system is based on a ballot machine, where, when we press the button with the election symbol, voting is done[1]. Here there is a security risk; the person voting may be a fake person vote. People out there might not know that someone is using Fake voting card, it can cause trouble. Electronic voting system security can be enhanced by using Biometrics. Biometrics is measurement and statistical Analysis of a person's unique physical and behavioral features. There are many techniques in biometrics such as Facial Recognition, Finger Print, Iris Recognition, Hand Geometry, Palm veins, palm impressions etc. Face recognition and fingerprints are used in this technique. Facial recognition is a biometric way of identifying someone Person by comparing live capture or digital image data Image data stored for that person. Finger print recognition Refers to the method of identification and confirmation of Identification of a person on the basis of comparison of two fingerprints (Finger print and sensed finger print in database) and is used for Certification in computerized systems[2].

EXISTING VOTING SYSTEM

Follows the principle of existing voting process Electronic Voting Machine (EVM) which has a simple design, Reliability and fast access characteristics. Unfortunately due Hardware problems in EVMs, malfunctioning of officers and invalid votes are being cast by invalid voters, and the same a person can vote multiple times. Must provide voting system Results are quick, but current voting system takes a long

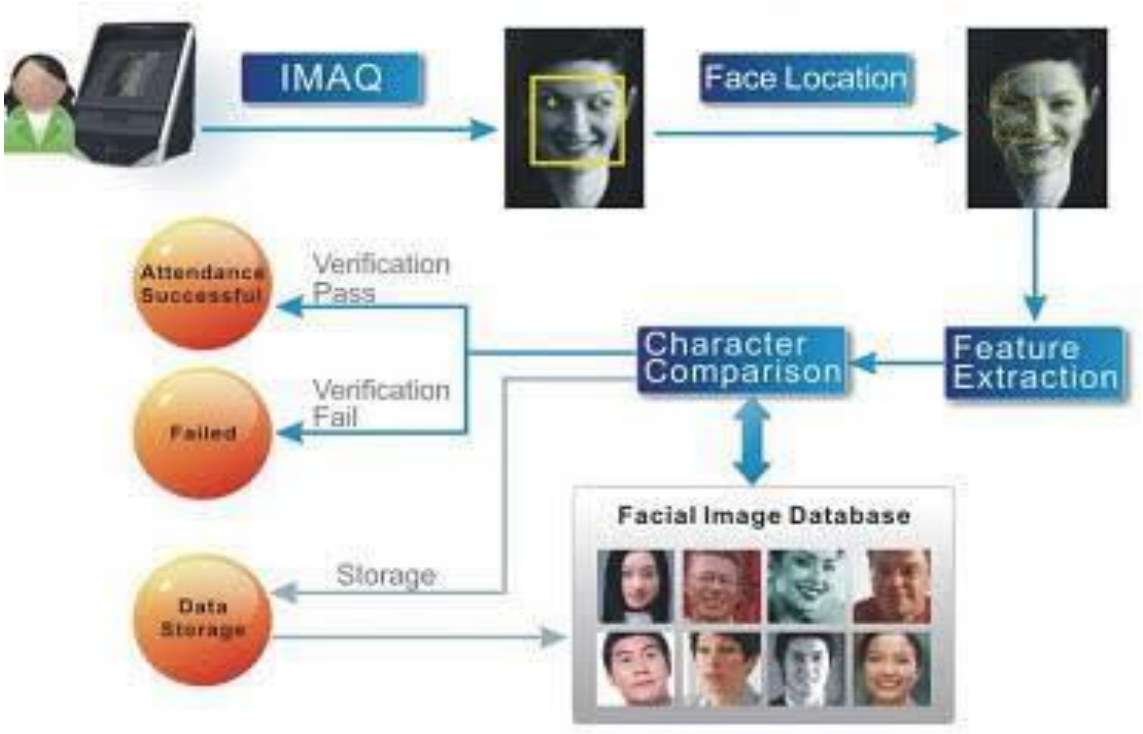
time generate results. Unimodal biometrics like finger print have many drawbacks like fingerprint will be taken so dirt will go inside finger, grease and other contaminating material will be will be recorded and there will be a possibility of getting finger print denied. when a person has a mark on his finger or A person whose finger is amputated will be considered handicapped.

This paper offers conceptual solutions to vote fraud process through multimodal biometrics that helps enhancing security, which provides elimination of fraud High level authentication and takes less time to provide Result? Multi Modal Biometrics is a fusion of two or more Types of biometrics. Fusion will lead to higher accuracy Compared to face and finger print recognition systems Existing EVM System

THE PROPOSED / PROTOTYPE DESIGN

The proposed EVM system has two inputs, one of which is Face Image and the other is Finger Print. Initially, in the face recognition part, the webcam captures the face image and it is Processed as shown in Fig. 1. The area of the face will be detected using the Viola and Jones algorithm[3], which includes: There are three types that feature necklaces [4][5], Adaboost and cascading. Facial features detected Face image using HOG algorithm[6]. It includes two methods they are intensity based method and Facility based method. Intensity based method is used to extract Face intensity features and feature based method are used Find the magnitude and angle of the face[7].

Bio Matrices Face Recognition



Bio Matrices Face Recognition Process fig-1

Photographs of the person's face are taken at the time of enrollment and it will be stored in the database. Database images and the captured image is compared and the result is taken[8].

Finger Print Verification

Finger print image is taken from finger print module and compared to the fingerprint stored in the database[9].

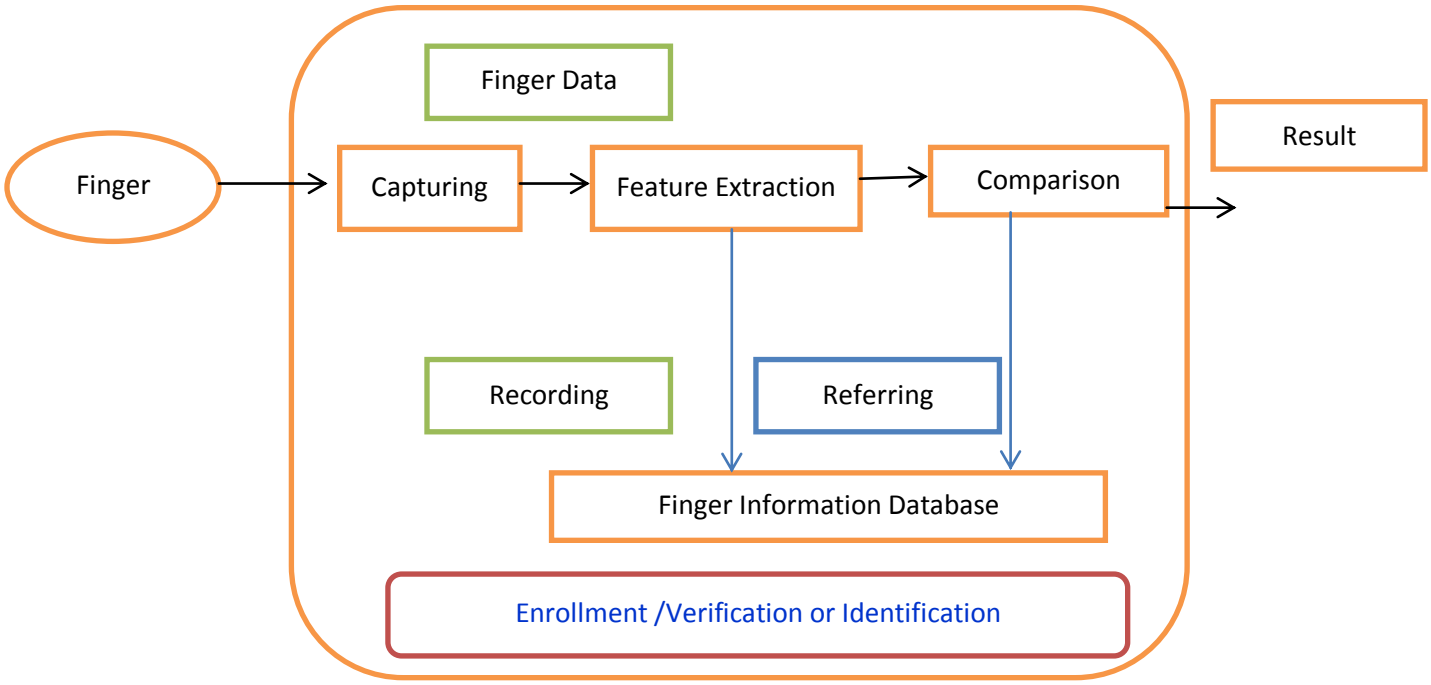


Fig -2 Finger Print Verification

Features of Face Module and Finger Print Module are connected as shown in next Figure 3 and the recognition result is given Matches microcontroller[10][11] and individual or Mismatch is displayed in the LCD display. Then that person One who is recognized will be allowed to vote.

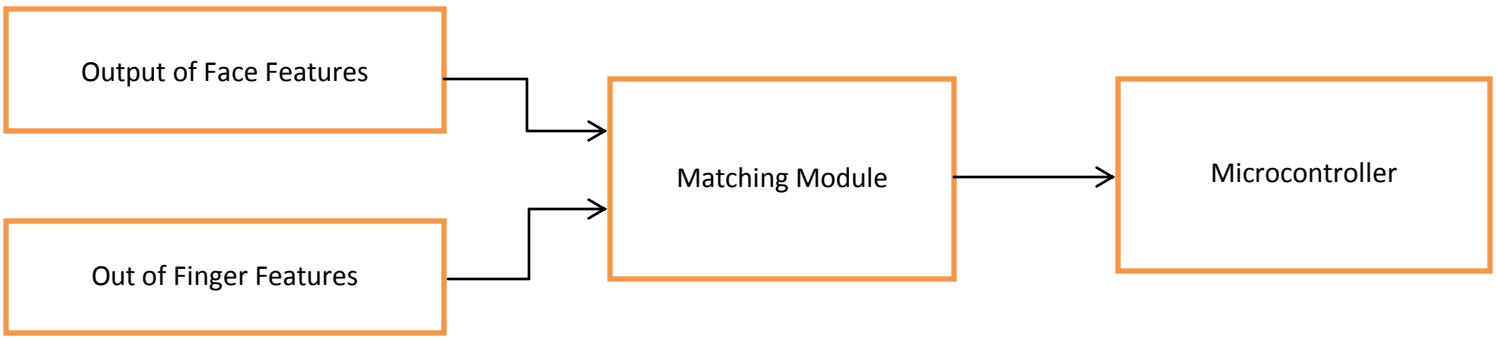


Fig. 3. Interfacing to the Microcontroller

LED display is used to display messages to the voter For example, select a candidate, vote accepted, matched, no matching etc. A buzzer is used to alert the user. the buzzer will If person comes to vote again, turn on, if not input match and if any misconduct occurs or if the person come again for voting. The figure below is a proposed block diagram for an electronic Voting system using biometrics[12].

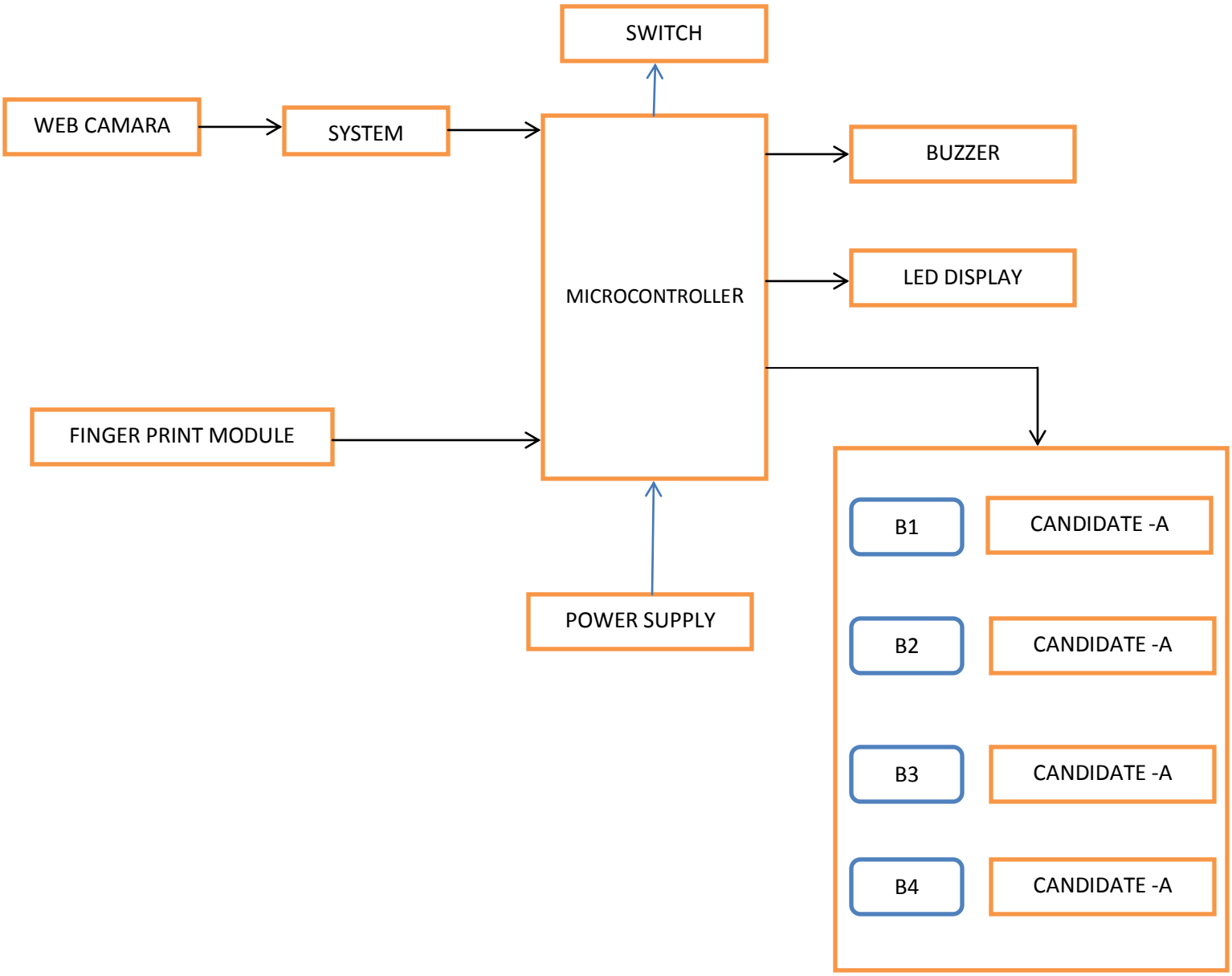


Fig. 4. Block diagram of proposed EVM

The switch can be operated in two modes which are Mode A and mode B. Mode A indicates that the switch is in voting mode and Mode B indicates that the switch is in counting mode. there will be votes Accepted only when the switch is in voting mode. B1, B2, B3 and B4 are the buttons used to represent the candidates. Voter press any one of these buttons. if the voter presses More than one button will buzzer at a time or first Pressing the button will be considered as a vote. Facial recognition is implemented using MATLAB.

Algorithm for the proposed design

Algorithm for the polling module:

Step 1: Put the Switch in Voting Mode

Step2: Capture face and finger print using web camera and finger print sensor.

Step 3: If both the inputs match then go to step (7)

Step4: If only one input will match and the other will not match Booth Chief will be empowered to decide whether the user is the user is the correct person or not

phase 5: The back head will enter the secret key, if it is correct He will check which biometric is not matching.

Step 6: If you don't turn on the LLC anywhere and the LCD will turn on will not be allowed to vote

Step 7: Voter will be allowed one button along with the blog's logo and the votes will be stored in Commemoration.

Step 8: If the voter PRESS more than 1 button the LCD will Display to press any one button and go to step (7).

Algorithm for counting mode

Step 1: Capture facial images and finger prints using web Camera and fingerprint sensor.

Step 2: If the inputs match, the authorized person will allowed to access and count the votes.

Step 3: If it does not match then go to step (1).

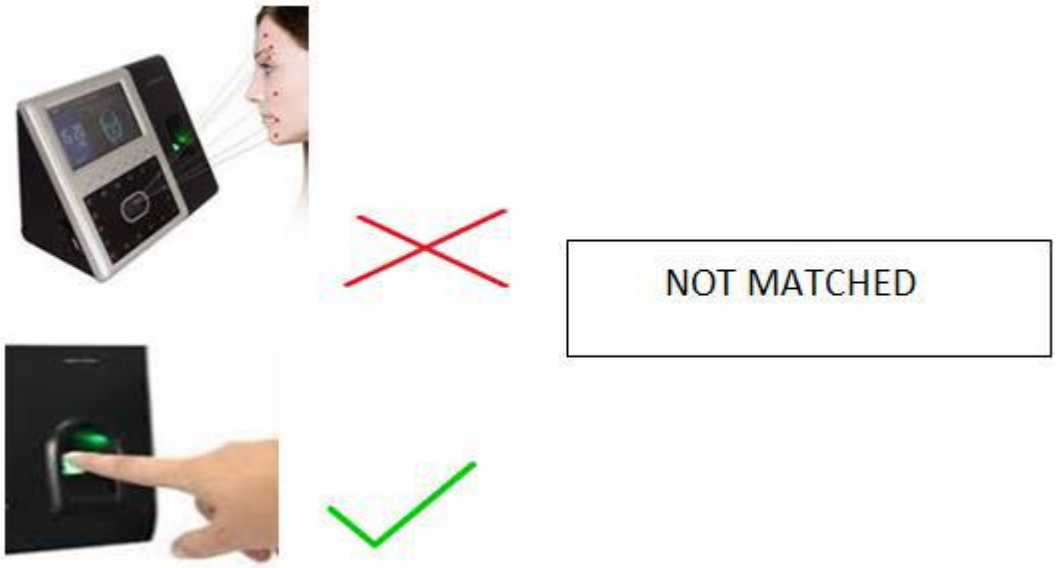
Step 4: The votes will be counted and displayed.

CASE STUDY

Case I: Both the inputs (face image, finger print) are matched

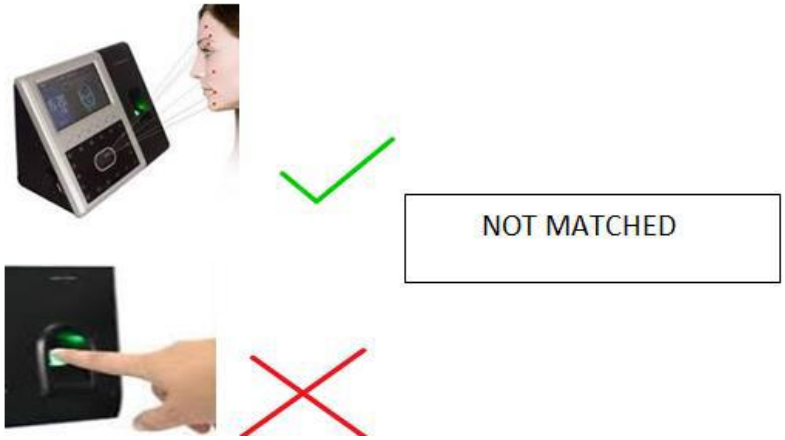
The LCD will display that the input has been matched, then it will Ask the user to vote by displaying the profile of the candidates.

Case II: Finger print matched but facial image does not match



The booth head will check whether the voter is a genuine person or not by checking the database. Voter will be allowed Vote up if it's the right person.

Case III: Facial image is matched but finger print is not matched the booth head will check whether the voter is a genuine person or not. Or not by checking the database. The tally is done and the person is allowed to vote.



If the voter is a genuine person then he/she will be allowed to vote

Case IV: Both inputs do not match

Alarm will be triggered and user will not be allowed to access until the booth chief approves his identity.

Case V: An unauthorized person comes to vote The alarm will go off to alert the authorities that it is counterfeit Person.

RESULTS AND DISCUSSION

- To create a database:
  To enroll the person's database, initially we will take his/her finger Prints and facial images.

- Fingerprint Recognition:
  LCD will display to place finger to take finger print and press switch 2 and if it matches the LCD will display as finger Matched and go with facial recognition.

- Face recognition:
  To take images of a face the LCD will display that it is a face matched and the person is allowed to vote.

- Voting Phase:
  Any one of the four switches will be pressed and the LCD will turn on Display that the vote has been accepted.

- Counting Phase:
  Authorized person will count the votes with his finger Print and result will be displayed.
  The false acceptance ratio is very low and the false rejection ratio is Very high. So, the system is time efficient.

CONCLUSION

In the proposed task, the numbers of faces of the person and Finger print is considered for performance analysis face the features are extracted with the Hogue algorithm have finger print Captured from the fingerprint sensor. Facial fusion and Fingerprint has been identified is a recognized person allowed to vote. is implemented using the voting module microcontroller results show proposed The method provides highly secure voting technology.

FUTURE SCOPE

Fewer numbers in the proposed voting prototype model Finger print can be stored in finger print module can be increased. This could be an electronic voting machine Interfaced with machines at various locations for the state elections so that the votes can be counted easily can time stamp should be provided so that there is no malpractice and provide More Security.

REFERENCES

[1] M. Janarthanan, A. Raghunath, S. Aiswarya, and E. Sajitha, "Smart voting machine based on finger print and face recognition," *AIP Conf. Proc.*, vol. 2405, no. 09, pp. 1–4, 2022, doi: 10.1063/5.0072707.

[2] P. G. Student, C. O. E. T. Sipna, and C. O. E. T. Sipna, "A review on smart voting systems 1 1 2," vol. 10, no. 4, 2022.

[3] P. Katta, O. A. Mohammed, K. Prabaakaran, M. Divya, G. Jayashree, and D. Keerthika, "Retraction: Smart voting using Fingerprint, Face and OTP Technology with Blockchain," *J. Phys. Conf. Ser.*, vol. 1916, no. 1, 2021, doi: 10.1088/1742-6596/1916/1/012139.

[4] A. Olumide S., B. Olutayo K., and S. E. Adekunle, "A Review of Electronic Voting Systems: Strategy for a Novel," *Int. J. Inf. Eng. Electron. Bus.*, vol. 12, no. 1, pp. 19–29, 2020, doi: 10.5815/ijieeb.2020.01.03.

[5] A. K. Tyagi, T. F. Fernandez, and S. U. Aswathy, "Blockchain and Aadhaar based Electronic Voting System," *Proc. 4th Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2020*, pp. 498–504, 2020, doi: 10.1109/ICECA49313.2020.9297655.

[6] S. Risnanto, Y. B. A. Rahim, N. S. Herman, and A. Abdurrohman, "E-Voting readiness mapping for general election implementation," *J. Theor. Appl. Inf. Technol.*, vol. 98, no. 20, pp. 3280–3290, 2020.

[7] A. V Nikam, P. C. Shetiye, and S. D. Bhoite, "Fostering Innovation , Integration and Inclusion Through Interdisciplinary Practices in Management A Critical Study of Electronic Voting Machine (EVM) Utilization in Election Procedure," no. March, pp. 1–3, 2019.

[8] K. Srikrishnaswetha, S. Kumar, and M. Rashid Mahmood, *A Study on Smart Electronics Voting Machine Using Face Recognition and Aadhar Verification with IOT*, vol. 65, no. July. Springer Singapore, 2019. doi: 10.1007/978-981-13-3765-9_10.

[9] Karthik G Maiya, Vineesha. T, Veena G, and Sujay S.N., "Secured Electronic Voting System using Biometrics," *Ncesc -2018*, vol. 6, no. 13, pp. 1–5, 2018.

[10] V. Kiruthika Priya, V. Vimaladevi, B. Pandimeenal, and T. Dhivya, "Arduino based smart electronic voting machine," *Proc. - Int. Conf. Trends Electron. Informatics, ICEI 2017*, vol. 2018-Janua, pp. 641–644, 2018, doi: 10.1109/ICOEI.2017.8300781.

[11] S. Chauhan, M. Jaiswal, and A. K. Kar, "The acceptance of electronic voting machines in India: A UTAUT approach," *Electron. Gov.*, vol. 14, no. 3, pp. 255–275, 2018, doi: 10.1504/EG.2018.093427.

[12] J. H. Mtepa, I. A. Akintola, A. S. Muftah, and A. Hussain, "The Evaluation of the Electronic Voting System : a Review," vol. 7, pp. 860–863, 2018.