



## **A SECURE HYBRID BIOMETRIC BASED E-VOTING SYSTEM FOR ELECTION PROCESS**

**J. Padmavathi**, Student, ECE, NRI Institute of Technology, Vijayawada

**M. Jahnavi**, Student, ECE, NRI Institute of Technology, Vijayawada

**M. Hemanth**, Student, ECE, NRI Institute of Technology, Vijayawada

**Dr. S.V. Rama Rao**, Associate Professor, Department of ECE, NRI Institute of Technology, Vijayawada

**Dr. R. Sunitha**, Professor & HOD, Department of ECE, NRI Institute of Technology, Vijayawada

### **ABSTRACT**

In early days the voters used paper ballots and hand tallying in India. Due to fraudulent voting and booth taking, where party supporters seize booths and cram them with pre-filled phoney ballots, this paper ballot technique is heavily criticized. In order to reduce these fraudulent votes, the electronic voting machines was introduced in the 20<sup>th</sup> century, it is widely used for voter identification. In Electronic Voting Machines (EVMs) the single parameter is used for the voter identification that might be voter ID or Aadhar which will be manually verified. To overcome this problem, a new technique which is based on three authentication techniques is proposed. The cross verifications provide more precision than a single parameter identification of a voter during an election technique. Initially, voter is verified by RFID card, and then he is authenticated by both fingerprint and face. As the system uses biometric authentication methods, if anyone of them is not matched then the voter is not allowed to vote.

**Keywords:** *Ballots, Biometric, EVM, Face, Fingerprint, RFID, Voter Identification.*

### **1.INTRODUCTION**

A country's inhabitants are given the ability to choose which members of the parliament to elect. A traditional way to complete the task is through an electoral system that uses paper ballots. The names of winners and losers are announced on radio and television over a long period of time using this manner. However, this method has certain problems, including increased costs, a longer processing time for voting, and mostly fraudulent voting and booth capturing. In order to reduce these fraudulent votes, electronic voting machines are introduced. In this EVMs only single parameter is used for voter identification that might be Aadhar or Voter identification, this EVMs are easily hacked. To overcome this problem A Secure Hybrid Biometric E-Voting system is proposed. Biometric authentication uses unique physical characteristics, such as fingerprint and face recognition, to confirm the identity of the voter. By lowering the risk, this technique aims to improve voting's accuracy, security, and efficiency of fraud voting. This voting system prevent fraud and double voting. Biometric data is unique to each individual and difficult to replicate, so if someone tries to vote under a different name, their biometric data would not match.

### **2.EXISTING ELECTRONIC VOTING SYSTEM IN INDIA**

With the current arrangement, a machine that electronically records votes are provided for every session. The officials at the poll booth press the big blue "Ballot" button to allow the voter to cast one vote. The voter presses the button next to the name and symbol of their favored candidate. Once the vote is cast the poll booth Officials has to press the "Ballot" button again for the next vote. The officials can use buttons close button to end the balloting and send the machine to have the votes counted. The officer in charge is given control of the current system and is responsible for ensuring that candidates are eligible to vote. Finally, gather every voting machine in one location before conducting the count.

### 3. PROPOSED HYBRID E-VOTING SYSTEM

In the proposed system three verification techniques are used such as RFID, Fingerprint and Face Recognition-based method are used for the voter identification. By using three techniques delivers greater accuracy than a single parameter identification method throughout an election procedure. When person is going to vote first scan the RFID card, Fingerprint and face capture. If these three are matched then only the person is allowed to vote.

The Block diagram of E-Voting System, the components are ATMEGA328p, RFID reader, Fingerprint scanner, Esp-32 Cam, 20\*4 LCD, 16\*2 LCD, Speaker and Voting section. In this block diagram ATMEGA328p Micro controller is the main component to interconnect the Inputs and Outputs. Here Power supply, RFID reader, Fingerprint scanner, Esp-32 cam, voting section and Voice Module, all these are connected on the input side and the output components are 20\*4 LCD, 16\*2 LCD, Speaker. in the voice Module there are 8 channels in this project we only use 4 channels, in that voice Module voice is recorded, that voice is come from the speaker, in between voice module and speaker an amplifier is connected it is used to increase the signal strength. Here we are using the RFID reader. It is used to read the details of the voter like Aadhar number, name.

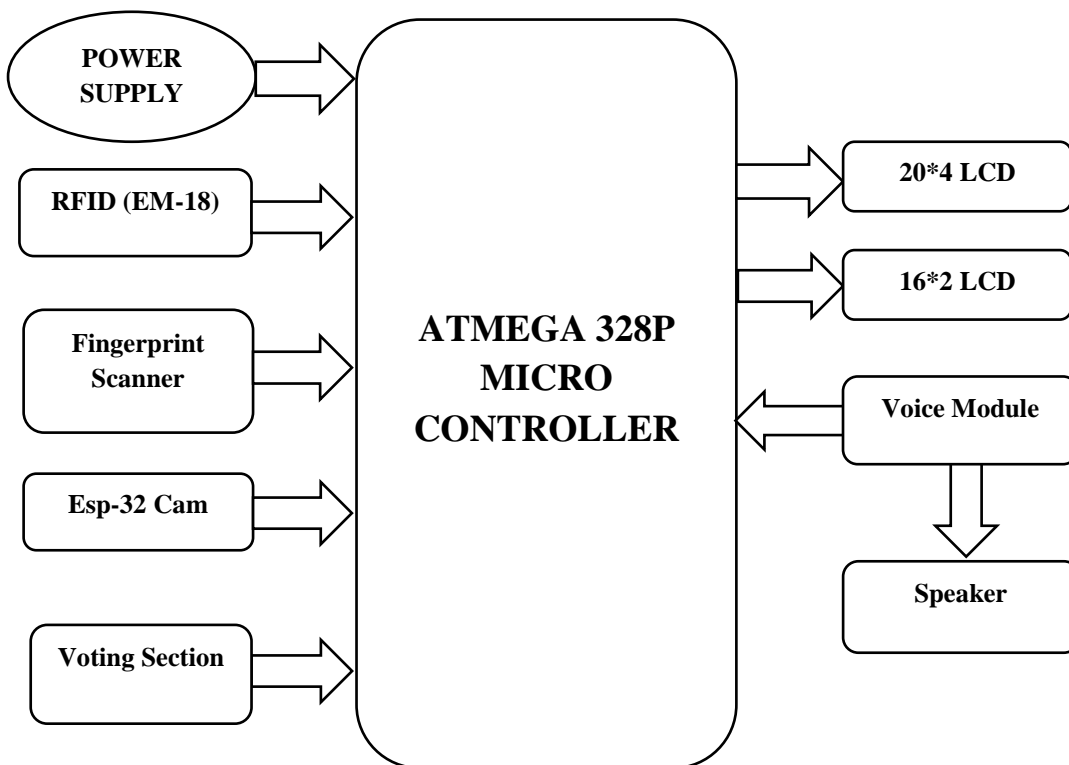


Fig.1 Block Diagram of E-Voting System

### 4. RESULTS AND DISCUSSION

Initially Power is connected to HBEV system, the 20\*4 LCD display title of the project after that voice come out from the speaker.



**Fig.2 Power Supply is Connected**

Step-1: After giving power supply, 20\*4 LCD displays please scan your Voter ID and simultaneously voice comes out from the speaker. In Voice Module there are eight channels we use 4 channels for this project. In the first channel voice recorded is please scan your Voter ID, by recording the voice is very helpful for who are unable to study in the LCD display.



**Fig.3 LCD Display Before Placing the Voter ID**

Step-2: As shown in figure 4 with the help of 20\*4 lcd display and speaker the voter scans his voter id proof. After scanning the voter ID, voter details are shown in the 20\*4 lcd display like voter name and Aadhar number.



**Fig.4 LCD Display After Scanning the Voter ID**

Step-3: As shown in figure 5 if in case voter scan the invalid ID. the 20\*4 lcd display shown the please scan valid ID proof.



**Fig.5 LCD Display Invalid Voter ID is Scanned.**

Step-4: As shown in figure 6 after scanning the ID proof, second step scanning the fingerprint of the voter. In the 20\*4 lcd display shown the please scan your fingerprint and With the help of voice Module, voice out from the speaker. with these two the voter can easily place their finger in the fingerprint scanner.



**Fig.6 LCD Display Before placing the Finger**

Step-5: As shown in figure 7 after scanning the fingerprint the 20\*4 lcd display if voter finger matches it show fingerprint ok, Please scan your face. If finger not matched then that person is not allowed to vote and also 20\*4 lcd display show error message like fingerprint not matched.



**Fig.7 LCD Display After Scanning the Finger**

Step-6: As shown in figure 8 After scanning fingerprint next step is scanning face, the 20\*4 LCD display instruction please scan your face and same instruction voice come out from the speaker. Voter scans his face with the help of Esp-32 Cam.



**Fig.8 Voter face is Scanning**

Step-7: As shown in figure 9 after successful completion of three verifications then power comes to voting section. the voting section uses the 16\*2 LCD display instructions, in 16\*2 lcd display show vote for your favorite party.



**Fig.9 Now the voter is allowed to vote**

Step-8: As shown in figure 10 in voting section there are four parties, the voter votes his favorite party after successful completion of voting the 16\*2 lcd display show vote to party name and thank you.



**Fig.10 LCD Display After successfully voted**

Step-9: As shown in figure 11 after successfully voted. The final results can only see officials by pressing the result. Button Voting section uses the 16\*2 lcd display to show the results and instructions. After completion of voting 16\*2 LCD display results, by press the results button.



**Fig.11 LCD Display for Final Result of voting**

## 5. CONCLUSION

By using biometric identifiers, such as fingerprint and facial recognition the system can prevent voter fraud and impersonation while also making the voting process more convenient and accessible for all voters. Additionally, the integration of blockchain technology and artificial intelligence can further improve the system's accountability and accuracy.

## REFERENCES

- [1] Jacobs, B., and Oostdijk, M., "Electronic Voting System", Google Patents, 2002
- [2] Electronic Voting System is the title of a B.Sc. thesis from the BRAC University in Dhaka, Bangladesh's department of computer science and engineering, completed in January 2007. Bhuiyan, M.S., Hossain, M.R., and Rehman
- [3] "An Introduction to Electronic Voting Application to Single Transferable Vote" by J. Traore was published on Orange Labs in July 2014.
- Biometric Recognition: Problems and Possibilities, National Academies Press, 2010; Whither Biometrics Committee
- [4] "Electronic Voting System," Google Patents, 2002; Jacobs, B.; and Oostdijk, M
- [5] "Experiences with Electronic Vote: Problems and Solutions," 9th International Conference on Theory and Practice of Electronic Governance Proceedings, pages 406-407, 2016. Galdamez, N., Estrebou, C., Pousa, A., Rodriguez, I., S.R. Eguren, F. Chichi Zola, A. Pasini, and A.D. Giusti are among the authors.
- [6] "The Development of Voting: Study of Conventional and Electronic Voting," by M. Awad and E. L. Leiss
- [7] Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, Andrew Rabi-novich: Going Deeper with Convolutions. Computer Vision and Pattern Recognition.
- [8] M. Liang and X. Hu, Recurrent convolutional neural network for object recognition, 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). pp. 3367-3375, 2015.
- [9] P. Pinheiro and R. Collobert, Recurrent convolutional neural networks for scene labeling, Proc. 31st Int. Conf., vol. 32, no. June, pp. 8290, 2014.
- [10] W. Shen, X. Wang, Y. Wang, X. Bai, and Z. Zhang, DeepContour: A deep convolutional feature learned by positive-sharing loss for contour detection, in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, vol. 0712, pp. 3982-3991,