Biometric Electronic Voting Machine

S. B. Patil[1], Smita Yadav[2], Reshma Bhaigade[3], Manthan Yadav[4], Poonam Patil[5], Yash Jadhav[6]
[123456] *D.Y. Patil College of Engineering and Technology, Kasaba Bawada, Kolhapur*

patilsb2000@gmail.com, smitayadav274@gmail.com, reshmabhaigade2002@gmail.com manthanyadav30@gmail.com poonampatil892002@gmail.com

Abstract— The key components of the Biometric Electronic Voting Machine (BEVM) include a secure database of eligible voters, a biometric recognition system for voter authentication, and a user-friendly interface for casting votes. The biometric identification process involves the capture and verification of unique physiological or behavioral traits, such as fingerprints, iris patterns, or facial features. By linking each voter to a distinct biometric identifier, the system ensures that only legitimate voters can participate in the electoral process. The implementation of the Biometric Voting Machine promises several benefits, including the reduction of electoral fraud, the streamlining of the voting process, and the enhancement of public trust in the democratic system. The BEVM not only strengthens the authentication process but also provides a transparent and auditable record of votes cast. The integration of biometric technology in voting machines represents a significant step towards achieving a more secure, efficient, and trustworthy electoral system. This project contributes to the ongoing efforts to modernize electoral practices, ensuring that the democratic process remains robust and resilient in the face of evolving challenges. As societies continue to embrace technological advancements, the BEVM stands as a beacon for the future of secure and transparent elections.

Keywords **-** *Fingerprint recognition, electronic voting, Encryption, Database management, Fairness*

I. INTRODUCTION

In the pursuit of enhancing the democratic process and ensuring the integrity of electoral systems, the implementation of advanced technologies has become imperative. One such groundbreaking innovation is the BEVM. This proposed work aims to explore and develop a secure, efficient, and user-friendly biometric voting system that leverages cutting-edge technology to redefine the way we conduct elections. Traditional voting systems often face challenges such as identity fraud, ballot tampering, and logistical inefficiencies. Biometric voting machines address these concerns by incorporating biometric authentication methods, such as fingerprints or iris scans, to uniquely identify voters. This not only enhances the security of the electoral process but also streamlines the voting experience, making it more accessible and convenient for citizens.

The primary objective of the BEVM is to fortify the security of the voting process. By linking each vote to a unique biometric identifier, the system minimizes the risk of impersonation and electoral fraud. This ensures the accuracy and reliability of election results, fostering trust among citizens in the democratic process.

The proposed work aims to develop an intuitive and user-friendly interface that accommodates voters of all demographics. The incorporation of biometric data ensures a quick and efficient authentication process, reducing waiting times and enhancing overall voter experience. Usability studies will be conducted to ensure that the system is accessible to individuals with diverse technological literacy levels. To enhance transparency and accountability, the BEVM will be designed to provide real-time monitoring and reporting capabilities. Election officials will have instant access to data, allowing them to detect and address any irregularities promptly. This feature will contribute to the timely and accurate dissemination of election results.

The project acknowledges the dynamic nature of electoral systems and aims to design a BEVM that is scalable and adaptable to different election scenarios. Whether used in local, national, or international elections, the system will be flexible enough to accommodate varying requirements and regulations.

Recognizing the sensitivity of biometric data, the proposed work places a strong emphasis on data privacy and ethical considerations. Robust encryption measures and strict access controls will be implemented to safeguard voter information, ensuring compliance with legal and ethical standards.

II. METHODOLOGY

Before an election, eligible voters need to register with their biometric information. This usually involves capturing biometric data such as fingerprint the collected biometric

data is stored securely in a central database. The biometric data captured at the polling station is compared with the stored biometric data in the central database to ensure a match.

If the biometric data matches, the voter is authenticated, and they are allowed to proceed to the voting phase. Once authenticated, the voter can cast their vote using the electronic voting machine.

The electronic voting machine typically displays the list of candidates, and the voter selects their preferred candidate by pressing a button or using a touch button interface. The electronic voting machine records the vote securely and ensures the voter's choice is accurately captured. After the voting process is complete, the electronic voting machines transmit the results to a central server for compilation and analysis.

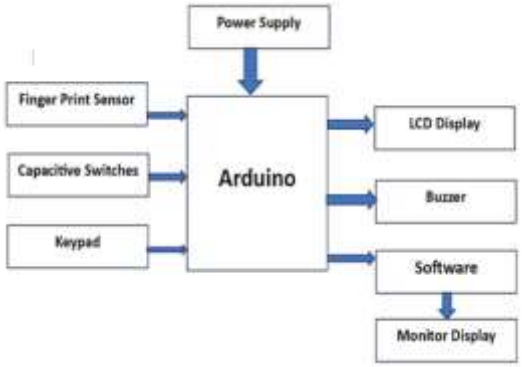

Fig:1 Block Diagram

1.Finger print scanner:

The fingerprint scanner captures the unique patterns and ridges of an individual's fingerprint using specialized sensors. If the captured fingerprint matches any existing template in the database, the voter's identity is verified. This verification process ensures that the person attempting to vote is the same individual registered in the system. Once the identity is authenticated, the individual is allowed to cast their vote.

2.Capacitive Switches:

Capacitive switches can be integrated into the user interface of the electronic voting machine to detect touch inputs from voters. When a voter touches a specific area on the interface, the change in capacitance due to the presence of the voter's finger is detected by the capacitive switch.

3.Keypad:

In a biometric electronic voting machine (EVM) project, a keypad may be included as part of the user interface. It is used for the purpose of Navigation.

4.LCD Display:

In a biometric electronic voting machine project, an LCD (Liquid Crystal Display) is often used to provide visual feedback to the user during the voting process. The LCD display is an essential component that allows voters to interact with the voting machine interface.

5.Buzzer:

In a biometric electronic voting machine project, a buzzer can serve as an essential component to provide audio feedback or alert signals during various stages of the voting process.

III. WORK FLOW OF PROJECT

Fig:2. Procedure for registration and Voting.

Database Creation-

The software that we are going to use for BEVM project is ‘Serial Studio’ In that project we have to create a database

for storage of all the information of candidates and voters, also the software will give all the information to track the voting data in a simplified way simplified manner.

It involves the following steps

i) Add the candidate in software-

Those candidates who wants to contest the election process, need to be added in our database.

ii) Add voters names in database-

The voter data is to be added and updated in a database.

iii) Storage of Fingerprints in database-

As, it is a biometric voting process we choose fingerprint for that, so we want to add fingerprints of all the voters in the database so that voting process will be done by matching this data.

iv) Scan the fingerprint-

As a first step of voting, we have to scan the fingerprints of voters.

v) Match fingerprint in database-

In registration process we have stored all the fingerprint data in the database, if anyone wants to vote he or she have to scan the fingerprint and the the sensor will take the picture and try to match the image with the database, if it found the image then only can do the further process of voting. Otherwise, the access is denied.

vi) Selection of candidates by capacitive switch-

If he or she is authorized voter then they have to give the vote by capacitive switch (Touch the switch).

After all these steps the registration and voting process will be completed. And all the data will be stored in the database, them simply we can access to the result by admin verification.

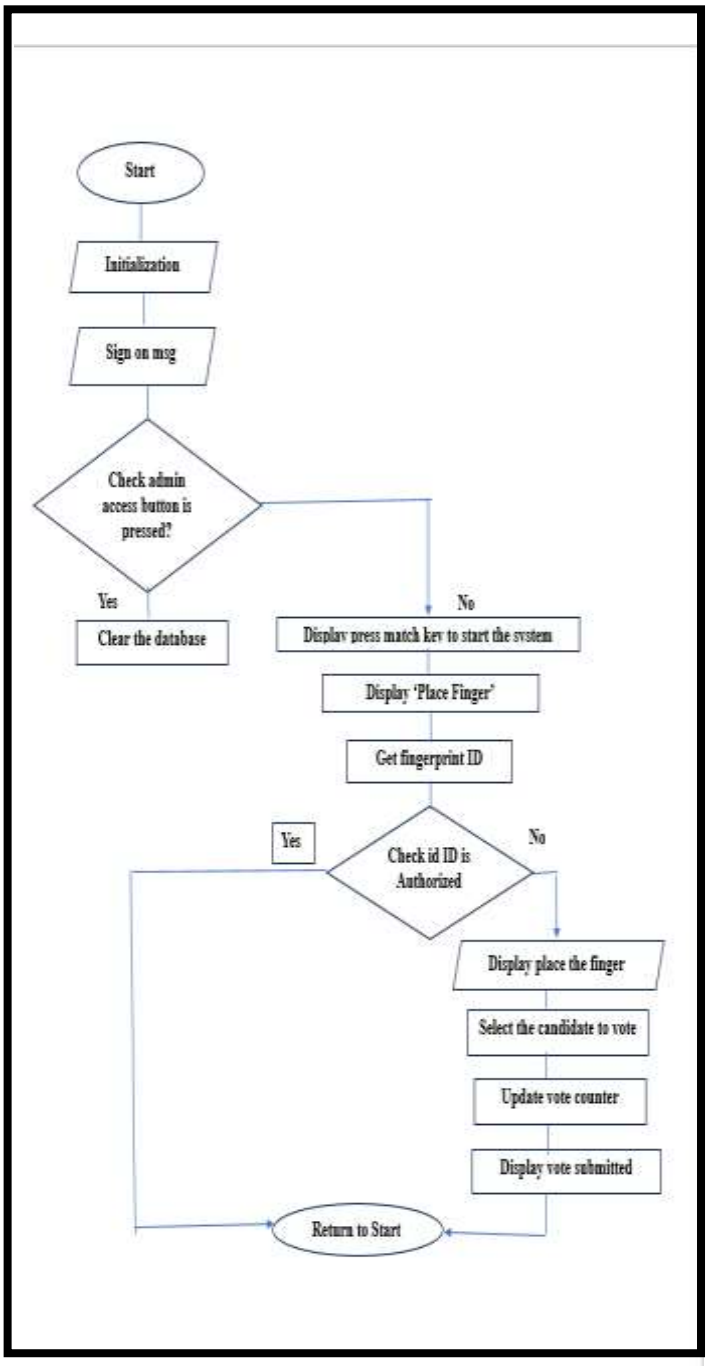

Fig.3. Flow Chart of System

IV. CONCLUSION

In conclusion, while biometric electronic voting machines offer significant benefits in terms of security, accuracy, and efficiency, their successful integration requires a

comprehensive approach. Striking a balance between innovation and addressing potential challenges is essential to ensure the continued improvement and trustworthiness of electoral processes using BEVMs.

V. REFERENCES

[1] Nikhil Chaudhari, Aditya Jambhale, Atharva Chourikar, Vijaya Chavan (2023). Electronic voting machine using Arduino with password encryption and poll control protection for unofficial elections. International research journal of modernization in engineering technology and science. Volume: 05/Issue: 03/March-2023.

[2] D. Ashok Kumar (2012) Electronic voting machine- A review, conference paper, international conference on pattern recognition, Informatics and Medical Engineering.

[3] Md. Murshadul Hoque (2014) A Simplified Electronic voting machine system. International journal of Advanced science and Technology.

[4] Dr. A. V. Nikam, Dr. P. T. Shetiye, Dr. S. D. Bhoite, (2019) A Critical study of electronic voting machine (EVM) Utilization in Election procedure. International journal of trends in specific research and development.

[5] Michael D. Byrne (2008). Electronic voting machines versus traditional methods: Improved preference, similar performance. Conference on Measuring, Business and Voting.

[6] Prof. Anisaara Nadaph, Ashmita Katiyar, Tushar Naidu, Rakhi Bondre, Durgesh kumari goswami. (2014). An analysis of secure online voting system. International Journal of innovative Research in computer science and Technology.Volume-2, Issue-5, September-2014.