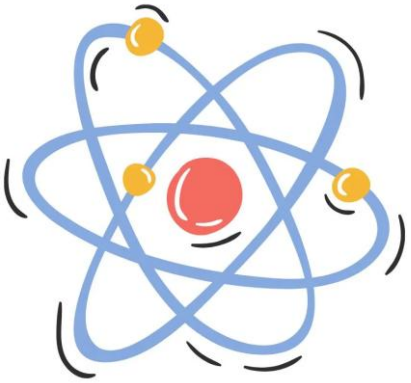


ISSN: 1672 - 6553

JOURNAL OF DYNAMICS AND CONTROL

VOLUME 10 ISSUE 03 2026: P281-286

INTELLIGENT BIOMETRIC VOTING SYSTEM WITH CAMERA VERIFICATION

Sanika Ghute, Omair Bhombal, Yashwant Jadhao, Prof. Jitendra Gaikwad

Department of Instrumentation and control engineering, Vishwakarma Institute of Technology Pune, Maharashtra, India

JOURNAL OF DYNAMICS AND CONTROL
https://doi.org/10.71058/jodac.v10i03012

INTELLIGENT BIOMETRIC VOTING SYSTEM WITH CAMERA VERIFICATION

Sanika Ghute[1], Omair Bhombal[2], Yashwant Jadhao[3], Prof. Jitendra Gaikwad[4]
Department of Instrumentation and control engineering, Vishwakarma Institute of Technology Pune, Maharashtra, India
[1]*sanika.ghute24@vit.edu,* [2]*omair.bhombal24@vit.edu,* [3]*yashwant.jadhao24@vit.edu,* [4]*jitendra.gaikwa@vit.edu*

Abstract: ***Elections that are free, fair, and transparent are a fundamental component of any democracy, which makes it necessary to ensure that the voting process is secure, transparent, and efficient. There are a number of challenges associated with traditional voting systems, including waiting time, the possibility of human error, manipulation, and delayed results. To overcome these problems, the proposed project introduces a smart voting machine, which ensures a safe, transparent, and efficient voting process using an electronic voting system. The system has been designed using an embedded system, a keypad, a camera module, and a display unit. The system ensures that every voter is verified before voting, thus preventing unauthorized access to the voting system. After the user is verified, he/she can proceed to vote by using the keypad, which ensures that the vote is recorded instantly. The system has a display unit that shows the user immediate feedback, while an alert system detects invalid votes. This approach enhances the overall efficiency, accuracy, and security of the voting process while reducing manual effort and operational costs. Due to its compact structure, low power consumption, and scalable design, the system can be effectively implemented in educational institutions, organizations, and small-scale local elections, ensuring a transparent and dependable voting mechanism.***

Keywords- Smart Voting Machine, Embedded System, Secure Authentication, Electronic Voting, Keypad Interface, Camera Module.

INTRODUCTION

In today's digital age, technology is crucial in nearly every part of human life, including communication, healthcare, banking, and governance. One significant democratic process that can greatly benefit from technology is voting. Elections are fundamental to any democratic system. It is essential to ensure they are fair, transparent, and efficient to maintain public trust. However, traditional voting methods, like paper ballots and manual vote counting, encounter several challenges. These include long processing times, human errors, high manpower needs, and the risk of manipulation or fraud. As populations grow and elections become more complex, these issues show the need for a more reliable and secure voting system. In response to these challenges, Smart Voting Machines have come up as a modern solution that combines embedded systems and digital technologies to improve the voting process. A Smart Voting Machine is an automated electronic system that accurately verifies voters, allows secure vote casting, and safely stores election data for result analysis.

These systems use components such as microcontrollers, authentication modules, cameras, sensors, and secure input interfaces. This setup ensures that only authorized voters can cast their votes and that each person votes only once. By automating the verification and vote-counting process, smart voting systems greatly reduce the

https://doi.org/10.71058/jodac.v10i03012

chances of human error and electoral fraud. Additionally, real-time data processing and monitoring improve transparency and provide instant feedback, making elections more trustworthy and efficient. Smart Voting Machines also reduce the reliance on large manpower, lower operational costs, and speed up both voting and result declaration. Their compact design and scalability make these systems suitable for educational institutions, private organizations, corporate decision-making, and small-scale government elections. Furthermore, using smart voting technology supports the vision of digital governance and smart city initiatives, promoting innovation, accountability, and efficiency in public administration.

1. LITERATURE SURVEY

Digital technology has significantly reshaped the way voting systems are designed and implemented, encouraging researchers to move away from traditional paper-based methods toward electronic and intelligent solutions. Early efforts in this domain focused mainly on automating the voting and counting process to reduce human error and improve efficiency. In 2014, Singh et al. [1] proposed a basic electronic voting machine using push buttons and a microcontroller, which simplified vote counting but lacked any form of secure voter authentication. Around the same time, Verma and Rao [2] introduced a microcontroller-based voting system with an LCD interface to display voting status and results; however, voter verification was still performed manually, limiting system security. Advancing this concept further, Kumar et al. [3] in 2016 developed a microcontroller-based electronic voting system that digitally stored votes in memory, eliminating issues such as paper ballot loss, duplication, and physical tampering, although the absence of identity verification remained a challenge.

To address authentication concerns, researchers began incorporating biometric and identification technologies. In 2017, Jain and Sharma [4] designed a fingerprint-based electronic voting system that ensured only authorized voters could cast their votes, effectively preventing impersonation and multiple voting. In the same period, Rahman et al. [5] proposed an RFID-based voting system in which voters were issued unique RFID cards for identification, significantly speeding up the verification process, though risks related to card loss and duplication were identified. Building on these ideas, Patel and Meena [6] in 2018 combined RFID technology with password-based authentication to create a multi-layer security system, enhancing protection against unauthorized access. Additionally, Gupta et al. [7] introduced a GSM-based voting system that transmitted voting-related information over mobile networks, improving transparency but introducing dependency on network availability.

With the emergence of the Internet of Things, voting systems became more interconnected. In 2019, Patil et al. [8] proposed an IoT-enabled smart voting machine capable of transmitting voting data to a central server in real time, allowing election officials to monitor the process remotely and improving transparency. During the same year, Chaudhary et al. [9] explored the use of wireless sensor networks for secure voting data transmission, reducing the need for extensive physical infrastructure while emphasizing the importance of strong encryption techniques. As system connectivity increased, attention turned toward secure data storage and accessibility. In 2020, Mehta and Shah [10] introduced a cloud-based voting system that stored voting data on remote servers rather than local devices, thereby minimizing the risks of hardware failure, physical damage, and data loss. Khan et al. [11] further highlighted the role of encryption, access control, and secure authentication in ensuring the reliability of cloud-supported voting platforms.

In subsequent years, researchers placed greater emphasis on usability and voter confidence. In 2021, Roy et al. [12] developed a graphical user interface that allowed voters to review and confirm their selections before final submission, significantly reducing accidental voting errors and improving user satisfaction. Supporting this approach, Nair and Joseph [13] emphasized that intuitive and user-friendly interfaces play a crucial role in increasing voter participation and trust in electronic voting systems. Security and integrity were strengthened further in 2022, when Ahmed et al. [14] implemented camera-based voter authentication by capturing images during the

https://doi.org/10.71058/jodac.v10i03012

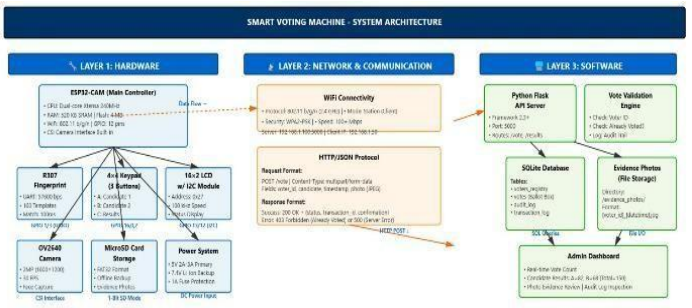
voting process to maintain visual records of voter participation. Similarly, Deshmukh et al. [15] proposed a multi-factor authentication system combining fingerprint and facial recognition technologies to enhance election security, while also acknowledging concerns related to privacy and data protection.

More recent studies have explored advanced technologies to ensure transparency and tamper resistance. Zhang et al. [16] proposed a blockchain-based voting system that ensured immutability and transparency of voting data through decentralized ledgers. Sharma and Iyer [17] demonstrated that blockchain technology could effectively prevent vote tampering and unauthorized data modification, although scalability and computational overhead remained significant challenges. Alongside these developments, system reliability and large-scale deployment issues were also examined. Almeida et al. [18] analyzed the impact of power failures on electronic voting systems and recommended backup power solutions to ensure uninterrupted operation. Kaur and Singh [19] investigated cyber-security threats in smart voting systems, emphasizing the need for intrusion detection mechanisms and regular software updates. Most recently, Wilson et al. [20] conducted a comprehensive review of smart voting systems deployed globally and concluded that while digital technologies significantly improve election efficiency and transparency, strong security frameworks, reliable infrastructure, and public awareness are essential for successful large-scale implementation.

2. METHODOLOGY

Building a Smart Voting Machine that actually works—one that checks all the boxes from your intro and the research—breaks down into three main steps: picking out the right hardware, writing the software, and then bringing it all together for testing. First up, hardware. Security and reliability are non-negotiable, so you start by choosing a solid microcontroller that can handle both cryptography and talking to other parts. For voter authentication, you can use either a fingerprint reader or an RFID reader, following what Jain and Sharma, or Rahman, suggested. This stops people from voting more than once. The interface needs to be clear and easy to use, so the plan is to go with a touchscreen GUI (thanks to Roy's advice), but a simple keypad works too. Votes get stored on a secure SD card or high-capacity EEPROM, always encrypted, just like Kumar recommends. You want this machine running no matter what, so it gets powered by a stable switching mode supply with a built-in UPS and battery backup. Want an extra layer? Add a camera module, like Ahmed's team did, to snap a photo during authentication as an audit trail. Next, it's all about programming. You write the firmware so the microcontroller fires up, checks the voter's fingerprint or RFID against a list, and only lets through the right people. Each vote is locked down with AES encryption, time-stamped, and hashed before it hits the SD card, making sure privacy and data integrity stay intact. Once someone votes, that's it—they can't go again. The software also runs the GUI, showing ballot options and instructions, and it's packed with error-handling, ready for anything from failed authentication to memory problems or a sudden power cut. The goal: no lost data, no mistakes. Finally, everything gets tested—thoroughly. With the hardware set up and the software loaded, you run it through its paces. Start with basic function: check that when someone casts a vote, the digital record matches exactly. Make sure the authentication module lets in only legit voters and keeps out fakes. See if regular people can actually use the interface easily. Then comes the real stress: security and reliability. Cast known votes and decrypt them to check for perfect accuracy. Try messing with the encrypted data to see if the system blocks or flags it right away.

3. ARCHITECTURE



4. DESCRIPTION OF COMPONENTS

https://doi.org/10.71058/jodac.v10i03012

1 Keypad:

A keypad lets people punch in numbers or letters—simple as that. In a smart voting machine, voters use it to pick their candidate. Each press sends a signal straight to the microcontroller, which logs the vote right away.

Fig.1. Keypad

2. **ESP Cam**

Then there's the ESP Cam. This little device comes with its own camera, so it can snap photos or check who's voting with face recognition. In a voting setup, it helps keep things secure. The machine checks each voter's face before letting them cast a ballot, so only the right people get through.

Fig.2. ESP Cam

3 Fingerprint Sensor R307:

A fingerprint sensor verifies the voter's identity by matching their fingerprint with the stored database. Only valid voters who have not voted before are allowed to vote, preventing fake and duplicate voting and improving election security.

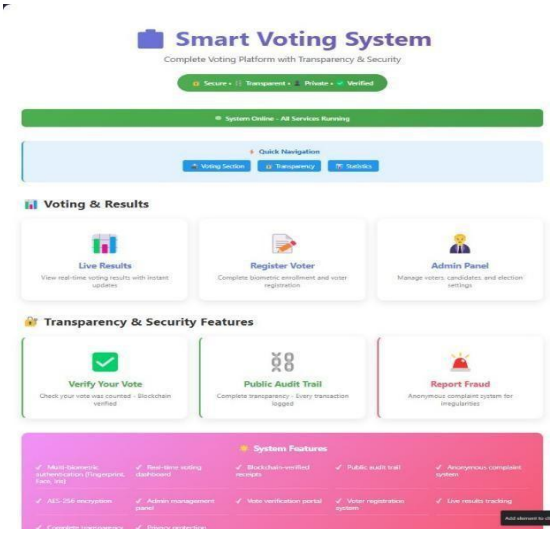
Fig.3.Fingerprint Sensor

4. 16×2 LCD with I2C Module:

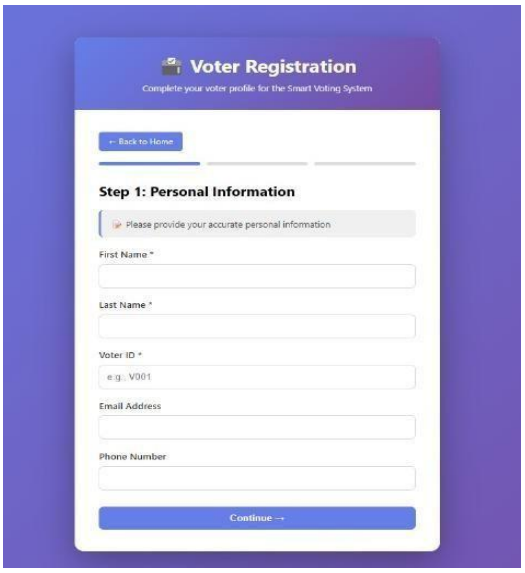
An LCD display is used to show instructions, candidate names, and confirmation messages to the voter. The I2C module simplifies wiring by using only two communication pins (SDA and SCL), making the system compact and efficient.

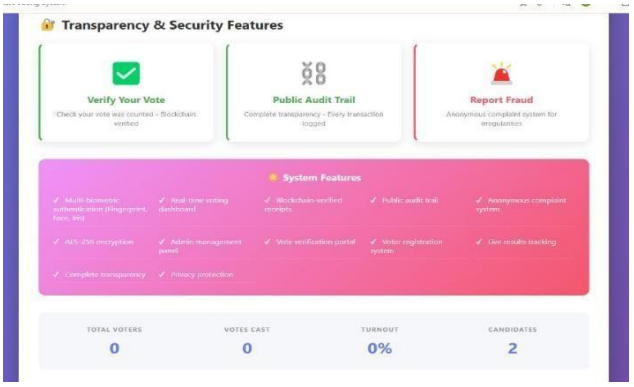
Fig.4 16×2 LCD with I2C Module

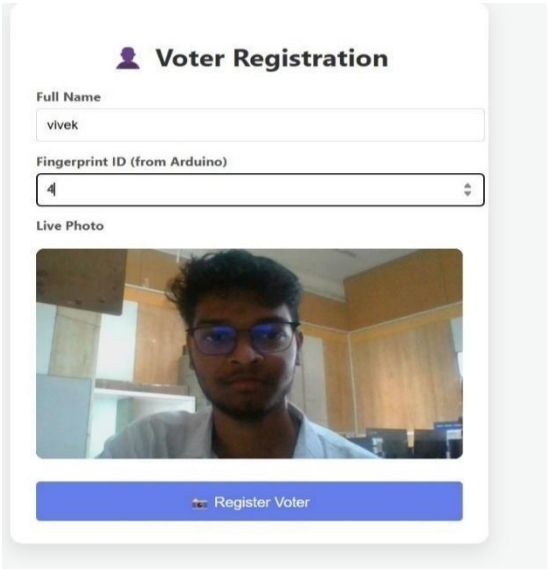
5. SIMULATION

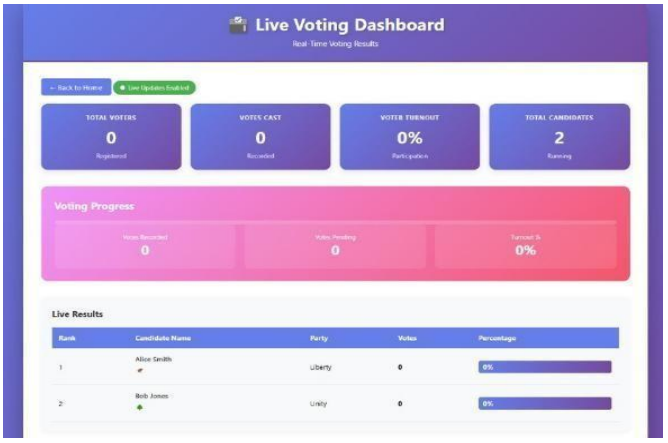


https://doi.org/10.71058/jodac.v10i03012

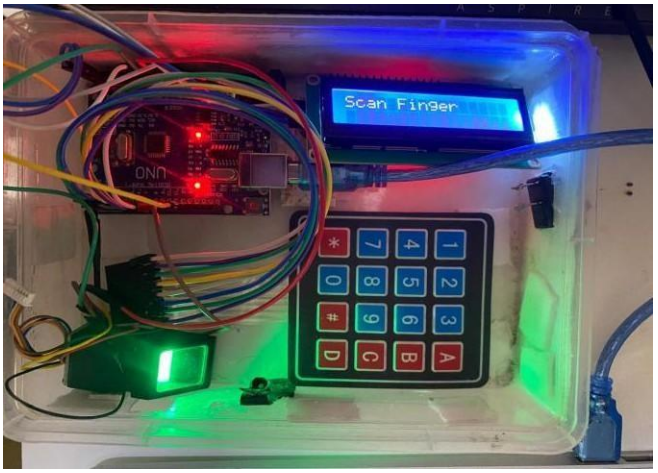


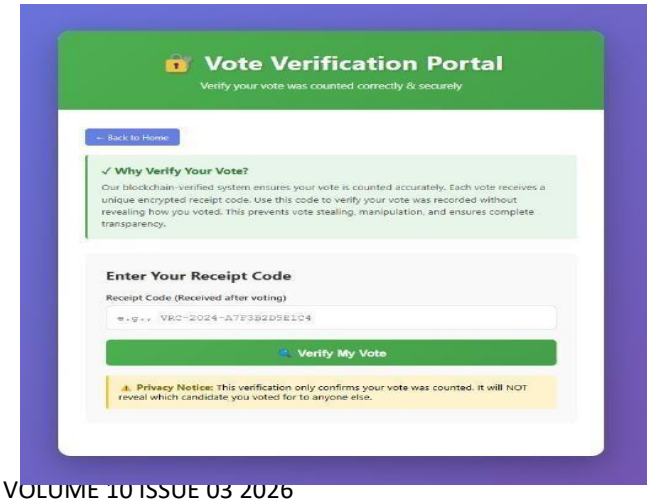






RESULT





CONCLUSION

The Smart Voting Machine system provides a secure, reliable, and efficient solution for modern elections. By using biometric authentication and

https://doi.org/10.71058/jodac.v10i03012

automated verification, it prevents fake, duplicate, and impersonation voting. The system reduces human error, increases transparency, and ensures that only eligible voters can cast their votes. Overall, the smart voting machine enhances trust in the election process and supports fair and accurate voting.

FUTURE SCOPE

IR sensors are installed in each parking space to detect vehicle presence. Servo motors are used at the entry and exit gates for automatic gate control. An I2C LCD displays the number of available parking spaces, and an SMPS powers all components including the Arduino Nano and sensors.The Arduino Nano is programmed to read IR sensor data, count occupied slots, and allow the entry gate to open only when parking space is available. The exit gate opens briefly when a vehicle is detected. The LCD updates the available slots in real time.All sensors and servos are tested and calibrated for accuracy, and the system is integrated and tested repeatedly to ensure reliable operation. This approach enables an automated, real-time smart parking system with minimal human involvement.

REFERENCES

[1] *International Journal of Engineering Research*, 2014.

[2] *International Journal of Computer Applications*, 2014.

[3] *International Journal of Advanced Research in Electronics and Communication Engineering*, 2016.

[4] *International Journal of Innovative Research in Computer Science*, 2017.

[5] *International Journal of Scientific & Engineering Research*, 2017.

[6] *International Journal of Engineering and Technology*, 2018.

[7] Gupta, R., Mishra, S., and Verma, A., "GSM Based Secure Voting System," *International Journal of Electronics and Communication Engineering*, 2018.

[8] *International Journal of Computer Science and Information Technology*, 2019.

[9] Chaudhary, R., Singh, M., and Kaur, G., "Secure Voting System Using Wireless Sensor Networks,"

[10] Mehta, D., and Shah, N., "Cloud Based Electronic Voting System," *International Journal of Cloud Computing*, 2020.

[11] Khan, S., Ali, R., and Ahmed, F., "Security Challenges in Cloud Based Voting Systems," *International Journal of Cyber Security*, 2020.

[12] Roy, A., Banerjee, S., and Das, P., "User Friendly GUI for Electronic Voting Systems,"

[13] Nair, V., and Joseph, L., "Impact of User Interface Design on Electronic Voting Systems,"

[14] *International Journal of Embedded Systems*, 2022.

[15] Deshmukh, P., Patil, R., and Joshi, S., "Multi-Factor Authentication Based Secure Voting System,".

[16] Zhang, Y., Liu, H., and Wang, X., "Blockchain Based Secure Voting System," *IEEE Access*, 2023.

[17] *International Journal of Blockchain Technology*, 2023.

[18] Almeida, J., Costa, R., and Silva, P., "Reliability Analysis of Electronic Voting Systems," *International Journal of Systems Engineering*, 2024.

[19] Kaur, J., and Singh, H., "Cyber Security Threats in Smart Voting Systems,"

[20] Wilson, T., Brown, L., and Martin, J., "A Review of Smart Voting Systems Worldwide,"