IJARSCT
ISSN: 2581-9429
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

Smart EVM Machine

Satyajit Yewale[1], Harshada Patil[2], Gayatri salunkhe[3], Athrav Shelar[4], Dr. B. P Kulkarni[5]
Student, Electronics & Telecommunication[1 2 3 4]
Assistant Professor, Electronics & Telecommunication[5]
Padmabhooshan Vasantraodada Patil Institute of Technology (PVPIT), Budhgaon, Sangli

Abstract: *This paper presents the design and implementation of a Smart Electronic Voting Machine (EVM) that ensures secure, reliable, and transparent voting. The proposed system integrates biometric authentication, real-time vote tallying, and secure data transmission using GSM/IoT. The Smart EVM aims to eliminate fraudulent voting practices, reduce manual intervention, and improve trust in the electoral process.*

Keywords: Smart EVM, Biometric Voting, IoT, GSM, Secure Election System

I. INTRODUCTION

A **Smart Electronic Voting Machine (EVM)** is an advanced version of the traditional electronic voting system, designed to enhance transparency, efficiency, and security in the electoral process. Unlike conventional EVMs, smart EVMs integrate modern technologies such as **IoT (Internet of Things), biometric authentication, GSM modules, and real-time data transmission** to ensure accuracy and prevent electoral fraud. These machines can be connected to a central monitoring system for live vote counting, voter verification, and tamper detection. With features like fingerprint scanning, camera surveillance, and digital display units, Smart EVMs aim to improve public trust and streamline the voting process in a more secure and user-friendly manner.

II. LITRATURE REVIEW

The evolution of Electronic Voting Machines (EVMs) has been a focal point of research in recent decades due to the increasing need for secure, efficient, and transparent electoral processes. Traditional EVMs, while instrumental in digitizing voting, have faced criticism regarding their vulnerability to tampering, lack of voter verifiability, and limited transparency. To address these concerns, several studies have proposed enhancements leading to the concept of Smart EVMs. These advanced systems incorporate technologies such as biometric authentication, blockchain for secure data handling, and IoT for real-time monitoring and reporting. According to various researchers, biometric integration, including fingerprint and iris scanning, can significantly reduce the chances of voter impersonation and fraud. Moreover, the implementation of the Voter Verified Paper Audit Trail (VVPAT) mechanism has been widely acknowledged as a step towards greater transparency, allowing voters to confirm their choices and enabling manual vote verification if needed. Literature further emphasizes the potential of blockchain-based Smart EVMs, which provide immutable records of votes, thereby strengthening electoral credibility. Several pilot projects and prototypes have demonstrated successful outcomes using these technologies in controlled environments. However, researchers also highlight challenges such as high infrastructure costs, digital literacy among voters, and the need for robust legal and ethical frameworks. In conclusion, the integration of smart technologies into EVMs promises a transformative impact on democratic systems by improving accuracy, accessibility, and public trust in electoral outcomes.

III. WORKING

The Smart Electronic Voting Machine (EVM) is an advanced version of the traditional voting system, integrated with modern technologies such as biometric verification, IoT, and real-time data transfer. The system begins by verifying a voter's identity using biometric fingerprint or Aadhaar-based authentication, ensuring that only eligible voters can cast their votes. Once authenticated, the voter selects their preferred candidate on a touchscreen or button interface. The vote is recorded electronically and stored in a secure memory unit. Simultaneously, a VVPAT (Voter Verifiable Paper Audit

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

Trail) system prints a slip as a confirmation, allowing the voter to verify their selection. The machine is also equipped with a control unit managed by polling officers to monitor the voting process. Additionally, some smart EVMs include features like GPS tracking, live status updates, and tamper detection to enhance security and transparency. This system ensures faster vote counting, reduces the risk of human error or tampering, and promotes a more reliable and efficient democratic process The block diagram of the Smart EVM (Electronic Voting Machine) illustrates the logical structure and functional interaction between key components of the system. At the core lies the **microcontroller unit** (typically an Arduino or similar embedded board), which acts as the central processing unit managing all system operations. The **fingerprint module** is connected to the microcontroller to authenticate voters using biometric data. When a voter places their finger on the sensor, the fingerprint is matched with pre-stored voter records. If authentication is successful, the system enables access to the **voting interface**,

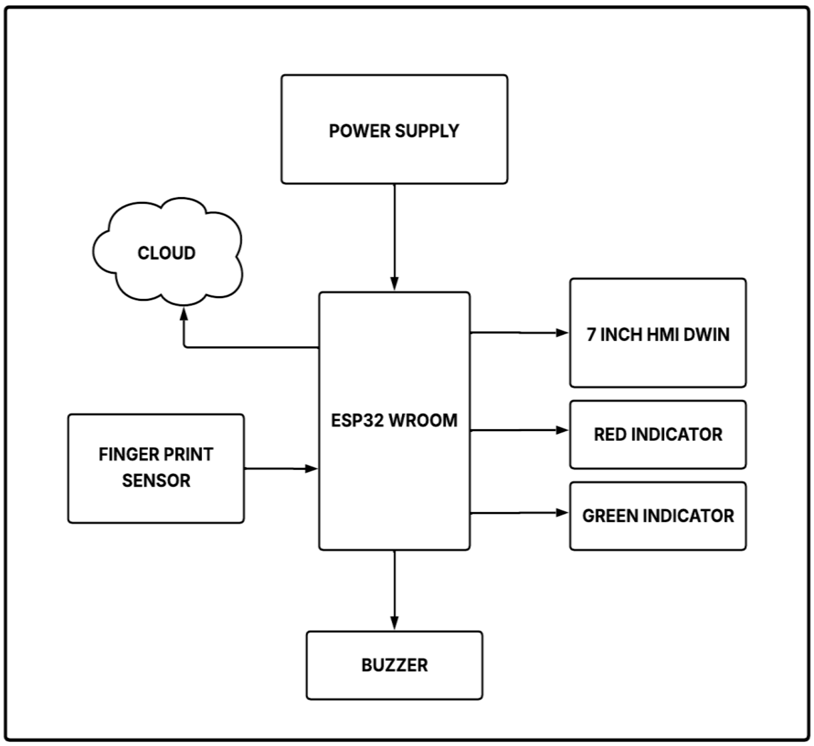

FIG : BLOCK DIAGRAM

can be a **touchscreen or button-based selection unit** allowing the voter to choose a candidate. Once the vote is cast, it is **encrypted and transmitted** via a **Wi-Fi or GSM module** to a **remote server or central election database**. The block diagram also includes a **display unit** (such as an LCD screen) to guide the voter through each step and confirm successful actions. For additional transparency and verification, a **VVPAT (Voter Verified Paper Audit Trail)** printer can be integrated to provide a printed slip showing the voter's selection, which is stored for audit purposes. The server component of the block diagram is responsible for **receiving, storing, and verifying the encrypted votes**. Additionally, a **monitoring and control unit** is included for real-time oversight and analytics. Power supply and security features such as tamper detection complete the system. The block diagram effectively demonstrates the integration of biometric verification, secure data transmission, and real-time monitoring, ensuring the reliability and transparency of the entire voting process

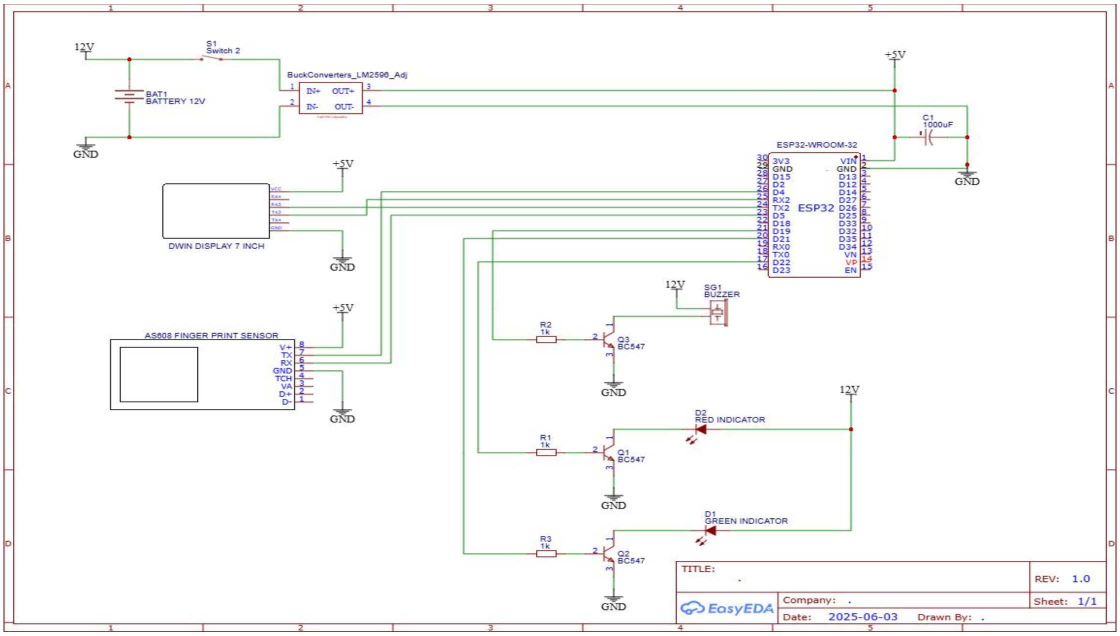

FIG. CIRCUIT DIAGRAM

The circuit diagram of a Smart EVM machine integrates both hardware and microcontroller components to ensure secure and efficient voting. The core of the system is an Arduino UNO or NodeMCU microcontroller, which controls all operations. Voters interact with the system via push-button switches (one for each candidate), and a 7-segment display or LCD shows the voting status or candidate ID. Each button is connected to a digital input pin of the microcontroller. When a voter presses a button, the microcontroller records the vote in memory (EEPROM or SD card). A 12V buzzer and LED indicators give feedback to the voter confirming the vote. For connectivity, especially in smart versions, Wi-Fi modules (like ESP8266) or GSM modules can be included for real-time vote count transmission to a central server. Power is supplied through a 12V DC battery, stepped down using a DC to DC buck converter to 5V/3.3V as required. Relay modules are optionally used for power control and tamper detection. The entire system is mounted on a custom PCB with clear circuit paths and labeled components

IV. SYSTEM REQUIREMENT

The implementation of a Smart Electronic Voting Machine (EVM) requires a well-structured integration of both hardware and software components to ensure secure, efficient, and user-friendly operation. On the hardware side, essential components include an Arduino microcontroller (such as Arduino Uno or Mega) for controlling the entire system, a fingerprint sensor module (e.g., R305 or GT-511C3) for biometric voter authentication, LCD or touchscreen display for the user interface, push buttons or a digital input mechanism for candidate selection, and Wi-Fi or GSM module (like ESP8266) to facilitate real-time vote transmission to a centralized server. Additional components such as power supply units, secure casing, buzzers or indicators, and printers (if VVPAT is included) are also required to support full system functionality. On the software side, the system needs a programming environment such as the Arduino IDE for microcontroller coding and web server/database backend using PHP, Python, or Node.js for managing and storing vote data. A cloud-based or local server is required to securely collect, store, and process vote records. The server should be equipped with encryption protocols (like SSL/TLS) to ensure secure communication and protect the integrity of transmitted data. The database, preferably MySQL or MongoDB, must be robust and capable of handling concurrent connections during the voting period. In addition, authentication algorithms, data verification routines, and error-handling protocols must be embedded to ensure system reliability. Together, these hardware and software components form a comprehensive ecosystem capable of delivering a secure, transparent, and tamper-resistant voting experience

DOI: 10.48175/IJARSCT-28147

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

V. HARDWARE REQUIREMENT

The Smart EVM machine requires a combination of electronic and embedded hardware components to function effectively. The main controller is typically an Arduino UNO, NodeMCU (ESP8266), or Raspberry Pi, which processes input and controls output devices. For voter input, push buttons are used—one for each candidate. Output components include an LCD or OLED display to show the voting status and a 12V buzzer and LEDs for feedback signals. A DC to DC buck converter is used to step down voltage for the microcontroller from a 12V battery or
3.7V 2600mAh Li-Ion battery. Data storage is achieved through an SD card module, and for smart connectivity, a Wi-Fi module (ESP8266) or GSM module is included. Additional components include a custom PCB, relays, resistors, foam sheet for insulation, and enclosures for safety and portability

1. 7-inch Dwin Display
2. ESP 32 WROOM S3
3. R307 Fingerprint sensor
4. 12 V/1Amp SMPS
5. 3.7V 2600mAh Li-Ion Battery
6. Indicator
7. 12v Buzzer
8. PCB
9. Foam Sheet 5mm

VI. SOFTWARE REQUIREMENT

The software requirements for a Smart EVM (Electronic Voting Machine) are designed to ensure secure, accurate, and user- friendly operation throughout the voting process. At the core, embedded firmware written in C/C++ or Micro Python runs on a microcontroller (such as the ESP32-WROOM-S3), handling real-time control of all hardware components including the fingerprint sensor, touchscreen display, buzzer, and indicators. A fingerprint matching algorithm is integrated to authenticate voters using biometric data captured by the R307 fingerprint sensor. The software must also include a graphical user interface (GUI), developed using platforms like DGUS Studio for the 7-inch DWIN display, which allows voters to view candidate details, confirm selections, and receive system feedback.

To ensure data security, the software should support secure data storage, either on EEPROM or SD card, with vote counts encrypted to prevent tampering. Additionally, access to administrative functions like result viewing or system reset must be password-protected. Optional communication modules may be integrated using protocols like UART, Wi-Fi, or Bluetooth for remote data transmission. The software should also include diagnostic tools for testing hardware functionality and a logging mechanism for tracking operations. Overall, the software must be efficient, reliable, and secure to support the integrity of the electronic voting process

Use of Thinger.io Platform for Live Vote Counting

In this project, Thinger.io, an open-source IoT cloud platform, was used to facilitate real-time data transmission between the hardware voting system and the cloud. The platform enabled continuous monitoring of vote counts, allowing instant updates on a user dashboard. Its seamless integration with microcontrollers and MQTT protocol allowed for efficient, accurate, and transparent vote tallying. This ensured that all data collected from the system was securely stored and displayed live on the Thinger.io interface, improving accessibility and visibility.

VII. CONCLUSION

In conclusion, the software component of a Smart EVM machine plays a critical role in ensuring a secure, transparent, and user- friendly voting process. It integrates various functionalities such as biometric authentication, real-time control, secure data handling, and interactive display interfaces. By combining reliable embedded firmware with user interface software and robust security measures, the Smart EVM system enhances the efficiency and integrity of electronic voting. Well-designed software ensures accurate vote recording, protects against tampering, and provides a seamless experience for both voters and administrators, making it a vital part of modern, technology-driven electoral systems

VIII. ACKNOWLEDGMENT

We would like to express our sincere gratitude to all those who supported and guided us throughout the development of the Smart EVM (Electronic Voting Machine) project. We are especially thankful to our project guide/mentor for their valuable insights, continuous encouragement, and technical support, which played a crucial role in shaping this project. We also extend our appreciation to our institution, faculty members, and lab staff for providing the necessary resources and a conducive environment for research and experimentation. Finally, we thank our peers and family for their constant motivation and support, without which this project would not have been possible.

IX. WORKING RESULT

REFERENCES

1. Fingerprint-based biometric smart electronic voting machine using IoT and advanced interdisciplinary approaches (E3S Web of Conferences, 2024)

• This academic article discusses a fingerprint-based voting system leveraging IoT for fairness in elections.

• Source:https://www.e3sconferences.org/articles/e3sconf/pdf/2024/37/e3sconf_icftest2024_0 1037.pdf?hl=en-IN

2. Online Voting System Project (Project Report - Hindustan University, 2024)

• This project report details an online voting system designed to be highly secure with a simple, interactive user interface.

• Source:https://www.researchgate.net/publication/380230553_Online_Voting_System