IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

ELECTRONIC ELECTION SYSTEM WITH BIOMETRIC CONNECTIVITY TO STRENGTHEN SECURITY & ELIMINATE MANUAL EVALUATION

[1]Mr.C.Md Aslam, M.Tech.,(Ph.D),Associate professor
[2]K.Vanaja, [3]N.Hemanth, [4]B.Deepika, [5]M.ChandraMohan Reddy, [6]M.Ushasree
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY
VIDYA NAGAR, PALLAVOLU (V), PRODDATUR-516360, Y.S.R (Dt.), AP

ABSTRACT

This study explores developing and implementing a novel Electronic Voting Machine (EVM) system integrated with biometric identifiers to enhance voting security and efficiency significantly. Traditionally, voting processes relied on paper ballots, a system fraught with several challenges, including over-voting, the loss or misplacement of ballot papers, environmental harm due to paper consumption, and a lengthy result compilation process. An advanced EVM system is proposed to address these issues, leveraging unique biometric identifiers - facial recognition and fingerprints - for voter authentication and secure vote recording. Our EVM system effectively improves the security against bogus voting and vote repetition, which have been significant concerns in previous voting systems. This robust approach to voter authentication minimizes the likelihood of voting fraud, thus contributing to a more reliable and secures voting process. However, the transition to this advanced EVM system is challenging. The study identifies key implications, including the impact on employment due to automation, potential inaccuracies and biases associated with biometric technologies, and vital privacy concerns surrounding using sensitive biometric data. Despite these challenges, the proposed system provides a substantial foundation for future enhancements. Opportunities for further development include the integration of additional biometric identifiers like finger recognition, refining the accuracy of current biometric technologies, and strengthening data privacy measures.

Keywords: Node MCU, Switch, LCD ,Buzzers, Fingerprint Sensor, and Power Supply etc.

I. INTRODUCTION

1.1 INTRODUCTION

Microcontroller are widely used in Embedded Systems products. An Embedded product uses the microprocessor (or microcontroller) to do one task & one task only. A printer is an example of Embedded system since the processor inside it perform one task only namely getting the data and printing it. Although microcontroller is preferred choice

ISSN 2347–3657
Volume 13, Issue 2, 2025

for many Embedded systems, there are times that a microcontroller is inadequate for the task. For this reason, in recent years many

manufactures of general-purpose microprocessors such as INTEL, Motorola, AMD & Cyrix have targeted their microprocessors for the high end of Embedded market. One of the most critical needs of the embedded system is to decrease power consumptions and space. This can be achieved by integrating more functions into the CPU chips. All the embedded processors have low power consumptions in additions to some forms of I/O, ROM all on a single chip. In higher performance Embedded system, the trend is to integrate more & more function on the CPU chip & let the designer decide which feature he/she wants to use.

1.2 EMBEDDED SYSTEM

Physically, embedded systems range from portable devices such as digital watches and MP3 players to large stationary installations like traffic lights, factory controllers, or the systems controlling nuclear power plants. Complexity varies from low, with a single microcontroller chip, to very high with multiple units, peripherals and networks mounted inside a large chassis or enclosure

In general, "embedded system" is not an exactly defined term, as many systems have some element of programmability. For example, Handheld computers share some elements with embedded systems such as the operating systems and microprocessors which power them but are not truly embedded systems, because they allow different applications to be loaded and peripherals to be connected. Embedded systems span all aspects of modern life and there are many examples of their use. Telecommunications systems employ numerous embedded systems from telephone switches for the network to mobile phones at the end-user. Computer networking uses dedicated routers and network bridges to route data.

EXAMPLES OF EMBEDDED SYSTEM:

Automated teller. machines (ATMS). Integrated system in aircraft and missile. Cellular telephones and telephonic switches. Computer network equipment, including routers timeservers and firewalls. Computer printers, Copiers. Disk drives (floppy disk drive and hard disk drive). Engine controllers and antilock brake controllers for automobiles. Home automation products like thermostat, air conditioners sprinkles and security monitoring system. House hold appliances including microwave ovens, washing machines, TV sets DVD layers/recorders. Medical equipment. Measurement equipment such as digital storage oscilloscopes, logic analysers and spectrum analysers. Multimedia appliances: internet radio receivers, TV set top boxes.Small hand-held computer with P1M5 and other applications. Programmable logic controllers (PLC’s) for industrial automation

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

and monitoring. Stationary video game controllers.

1.3 CHARACTERISTICS:

Embedded systems are designed to do some specific tasks, rather than be a general-purpose computer for multiple tasks. Some also have real-time performance constraints that must be met, for reasons such as safety and usability; others may have low or no performance requirements, allowing the system hardware to be simplified to reduce costs. Embedded systems are not always standalone devices. Many embedded systems consist of small, computerized parts within a larger device that serves a more general purpose. For example, the Gibson Robot Guitar features an embedded system for tuning the strings, but the overall purpose of the Robot Guitar is, of course, to play music. Similarly, an embedded system in an automobile provides a specific function as a subsystem of the car itself.

The software written for embedded systems is often called firmware, and is usually stored in read- only memory or Flash memory chips rather than a disk drive. It often runs with limited computer hardware resources: small or no keyboard, screen, and little memory.

1.4 MICROPROCESSOR (MP):

A microprocessor is a general-purpose digital computer central processing unit (CPU). Although popularly known as a “computer on a chip” is in no sense a complete digital computer. The block diagram of a microprocessor CPU is shown, which contains an arithmetic and logical unit (ALU), a program counter (PC), a stack pointer (SP), some working registers, a clock timing circuit, and interrupt circuits.

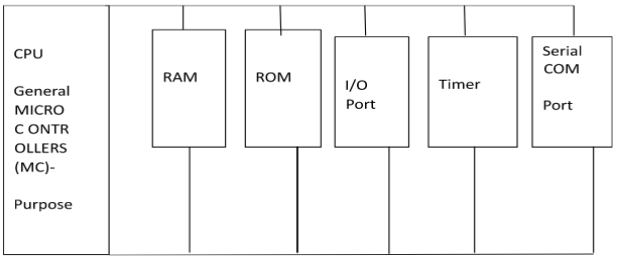


Fig 1.1 Block diagram of microprocessor

1.5 MICROCONTROLLER (MC):

Figure shows the block diagram of a typical microcontroller. The design incorporates all of the features found in micro-processor CPU: ALU, PC, SP, and registers. It also added the other features needed to make a complete computer: ROM, RAM, parallel I/O, serial I/O, counters, and clock circuit.

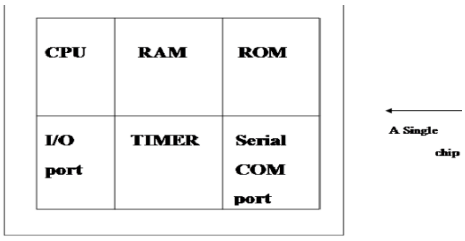


Fig 1.2 Microcontroller

1.6 COMPARISION BETWEEN MICROPROCESSOR AND MICROCONTROLLER

The microprocessor must have many additional parts to be operational as a computer whereas microcontroller requires no additional external digital parts. The prime use of

ISSN 2347–3657
Volume 13, Issue 2, 2025

microprocessor is to read data, perform extensive calculations on that data and store them in the mass storage device or display it. The prime functions of microcontroller is to read data, perform limited calculations on it, control its environment based on these data. Thus the microprocessor is said to be general-purpose digital computers whereas the microcontroller are intend to be special purpose digital controller. Microprocessor need many opcodes for moving data from the external memory to the CPU, microcontroller may require just one or two, also microprocessor may have one or two types of bit handling instructions whereas microcontrollers have many.

II. LITERATURE SURVEY

2.1 INTRODUCTION

Voting, in its most fundamental sense, is a means to express choice or preference from an array of options. It forms the backbone of democratic processes worldwide, deciding the leaders the populace entrusts with power. This fundamental democratic process has undergone various transformations throughout history, from traditional paper ballots to more advanced Electronic voting machines (EVMs). However, the shift from traditional paper ballot voting to EVMs has not been without challenges and consequences. Originally, the voting process involved the physical presence of each voter, the use of ballot papers, and manual counting – a method proven to be time-consuming and prone to inaccuracies and manipulation. Issues such as over-voting, where voters accidentally stamp more than once, and ballot papers being lost or miscalculated were significant challenges. These systemic problems, compounded with the environmental concerns around using paper, underscored the need for a more efficient and secure voting mechanism, hence the adoption of EVMs. Designed and developed in India, in collaboration with Bharat Electronics Limited, Bangalore, and Electronics Corporation of India Limited, Hyderabad, EVMs promised to alleviate many of these challenges. Offering advantages such as efficient vote recording, quick result processing, enhanced voter-friendliness, and a reduction in the use of paper, EVMs marked a significant evolution in voting technology. However, adopting EVMs has also raised concerns. The transition to an electronic voting system has reduced the need for manpower, potentially affecting employment during elections. Furthermore, questions about the security and integrity of the voting process in an electronic format remain. The present work aims to address these concerns and refine the current EVM system, utilizing biometric identifiers to strengthen security and integrity. By proposing the unique physical attributes of voters, such as facial recognition and fingerprint data, the study aims to establish an unhackable, accessible, and more reliable voting system. This paper details the methodology, discusses the outcomes and

ISSN 2347–3657
Volume 13, Issue 2, 2025

implications of the proposed system, and outlines future avenues for improving upon this novel application of biometric technology in voting systems..

III. PROBLEM STATEMENT

The automated vote systems are developed before some years ago one. The prevailing systems have alone been approved in some growth obtained countries. That too, not altogether developed countries. as a result of the protection has not however been totally preserved. We have a tendency to captive onto automation in the main to consider security. However, the prevailing systems didn't guarantee.

The existing system isn't terribly efficient and reliable and conjointly manual approaches are needed for verification, which consumes longer. At present, balloting unit and management unit are wont to conduct the option. Pick unit is employed by the elector to settle on the candidates whereas control unit is employed by the Polling officer to allow the user for option. But in the existing system, felonious option is feasible by the invalid elector that is sensitive to security attack, which ends that some people lose their right in choosing the government..

3.1 LIMTATION OF SYSTEM

Susceptibility to Fraud: Paper ballots can be easily manipulated, and traditional EVM can be tampered.

Manual Errors: Counting errors and mismanagement of ballots are common in manual systems.

Lack of Voter Verification: Traditional systems do not have strong mechanisms to verify voter identities, leading to potential multiple voting.

Transparency Issues: The process lacks transparency, leading to mistrust among voters..

IV. PROPOSED SYSTEM

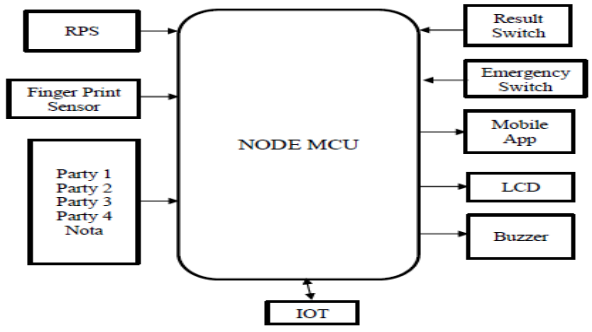
The system aims at developing a fingerprint based advanced Electronic Voting Machine (EVM) which helps in free and fair way of conducting elections which are basis for democratic country like India .This project consists of following units a Voting system, fingerprint module and ARM controller Unit. The voter first puts his finger on the fingerprint module which checks for the authentication of the user. If the voter is the authenticated one, he will now poll his vote in the voting system by simply pressing button against his favorite leader through a button. The control unit consists of a ARM controller, push button for different operations of EVM. The votes casted for particular candidate in that particular section of constituency is shown through an LCD display.To perform this intelligent task, Node MCU micro controller is loaded with an intelligent program written in embedded „C“ language.

4.1 BLOCK DIAGRAM OF PROPOSED SYSTEM

The voter places their finger on the fingerprint module.The module scans the fingerprint and compares it with the pre-stored database.If the fingerprint matches an authorized voter, access

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

is granted to proceed with voting.After authentication, the system enables the voter to cast their vote.The voter selects their preferred candidate party by pressing a dedicated button on the voting system.Once the vote is cast, the ARM controller records it securely in the system.The vote count for each candidate party is updated.The LCD display shows the total votes for each candidate in real time (or at the end of polling).The ARM controller manages the overall system, ensuring smooth operations.It processes voter authentication, registers votes, and maintains secure data storage.The controller is programmed using Embedded C for efficient execution.Only authenticated users can vote, preventing duplication or fraudulent voting.The NodeMCU microcontroller ensures secure data handling and communication.This system enhances the reliability and transparency of elections by integrating biometric authentication with an electronic voting system.



V. BLOCK DIAGRAM OF PROPOSED SYSTEM

HARDWARE COMPONENTS

The following hardware tools used in the proposed system

Power Supply, Node MCU, Finger Print Sensor, Switch, LCD, Buzzer

SOFTWARE COMPONENTS

The following software tools used in the proposed system : Arduino IDE, Proteus Design Tool

TECHNOLOGY USED

IOT

VI. RESULT AND DISCUSSION

PROTOTYPE

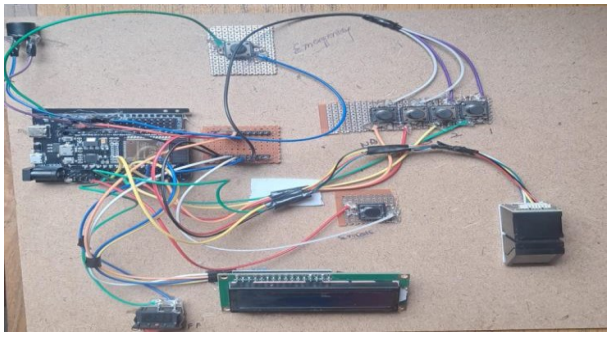


Fig: Prototype of our Project Kit

EXPERIMENTAL RESULTS

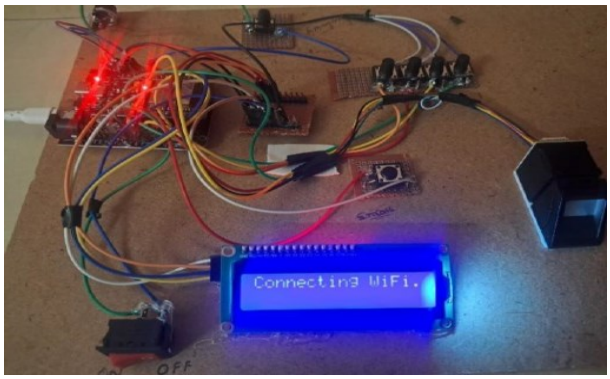


Fig:Connecting Wi-Fi to the kit

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

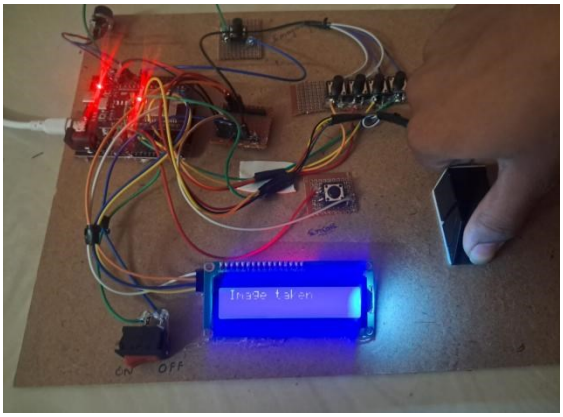


Fig:Image Taken from the voters

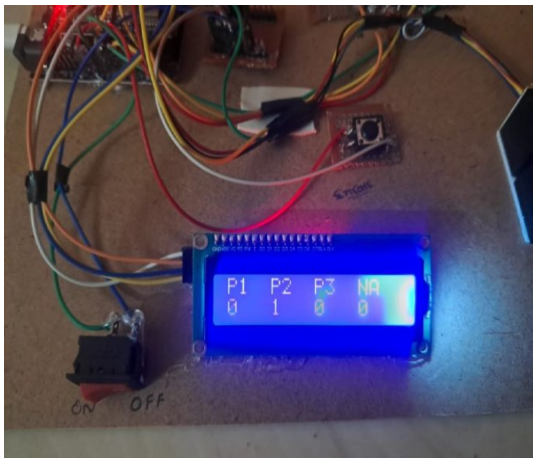


Fig:Real-time monitoring of voting Results

VII. CONCLUSION

The exploration and implementation of an electronic voting machine (EVM) system equipped with biometric identifiers have presented a new paradigm in the evolution of voting processes. The present work has shown that integrating unique biometric features like facial recognition and fingerprints into EVMs greatly enhances the system's security against bogus voting and vote repetition, thus making the voting process more reliable and secure.The adoption of EVMs has helped eliminate many of the issues associated with traditional paper-based systems, such as over-voting, loss of ballot papers, and environmental concerns around the use of paper.In addition, using EVMs has led to significant improvements in the efficiency of the voting process, with real-time vote tallying and quick result compilation

VIII. FUTURE SCOPE

Additionally, while biometric identifiers have improved the security and efficiency of the voting process, their use is not devoid of potential inaccuracies and biases. These technologies must be continually refined to prevent false rejections or acceptances and ensure they do not unfairly favor or disadvantage any particular group of voters.

Privacy concerns must also be considered, as biometric data is sensitive personal information. Moreover, the proposed system's success hinges upon the matching of voter details with a pre-existing database, a process that may encounter discrepancies or mismatches. Safeguards must address situations where valid voters cannot match their details, ensuring they are not denied their fundamental right to vote.As the system stands now, it significantly improves the voting process's security and efficiency..

REFERENCE

1.M. Khosla, "The possibility of modern India," Global Intellectual History, 2021.

2.A. Shah, "What if We Selected our Leaders by Lottery? Democracy by Sortition, Liberal Elections and Communist Revolutionaries,"

ISSN 2347–3657
Volume 13, Issue 2, 2025

Development and Change, vol. 52, no. 4, pp. 687–728, 2021.

3.A. Kud, "Decentralized Information Platforms in Public Governance: Reconstruction of the Modern Democracy or Comfort Blinding?," International Journal of Public Administration, vol. 46, no. 3, pp. 195–221, 2023.

4.D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, "Secure Online Voting System Using Biometric and Blockchain," Advances in Intelligent Systems and Computing, vol. 1042, pp. 93–110, 2020.

5.T. M. A. Elven and S. A. Al-Muqorrobin, "Consolidating Indonesia's Fragile Elections Through E-Voting: Lessons Learned from India and the Philippines," Indonesian Comparative Law Review, vol. 3, no. 1, pp. 63–80, 2021.

6.S. Agarwal, A. Haider, A. Jamwal, P. Dev, and R. Chandel, "Biometric based secured remote electronic voting system," 2020 7th International Conference on Smart Structures and Systems, ICSSS 2020, 2020.

7.A. Olumide, B. Olutayo, and S. Adekunle, "A Review of Electronic Voting Systems: Strategy for a Novel," International Journal of Information Engineering and Electronic Business, vol. 12, no. 1, pp. 19–29, 2020.

8.A. K. Tyagi, T. F. Fernandez, and S. U. Aswathy, "Blockchain and Aadhaar based Electronic Voting System," Proceedings of the 4th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2020, pp. 498– 504, 2020.

9.Balaji, Speech of Shri V S Sampath, CEC for Defence Estates Day Lecture 2014

10.R. Haenni, E. Dubuis, and U. Ultes-Nitsche, "Research on e-voting technologies." Bern University of Applied Sciences, Technical Report 5, 2008..