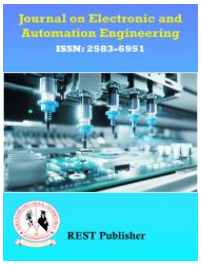
Journal on Electronic and Automation Engineering
Vol: 4(2), June 2025
REST Publisher; ISSN: 2583-6951 (Online)
Website: https://restpublisher.com/journals/jeae/
DOI: https://doi.org/10.46632/jeae/4/2/57



Fingerprint Based Electronic Voting Machine

***J. Suresh, P. Vishnu, S. Harinath, S. Fardeen**
Nalla Malla Reddy Engineering College, Hyderabad, Telangana, India
*Corresponding Author Email: suresh.ece@nmrec.edu.in

Abstract: *In a democratic country like India, voting is an important way where the citizen can cast their vote. Usually voting is done by casting their vote in polling booth. As the technology increases, nowadays electronic voting machine is used for casting vote. This paper is about an IoT based voting machine with fingerprint verification. The main aim of this project is to make voting secure using fingerprint verification and also to reduce malpractices. The details of the voter along with their fingerprint in stored in database. If the fingerprint matches with the stored fingerprint, the system checks the aadhaar number of the user and if authenticated, it checks if multiple votes have been cast. If the fingerprint matching is not correct "Matching failed" message will be displayed and if aadhaar number is not correct, then "Aadhaar not match" message will be displayed. Voter can enter his/her native place and vote for the corresponding candidate using thing speak and the result can be obtained using the same. The Arduino Uno is the controller used in this project. Fingerprint is used to authenticate the user. There is at least a slight difference between the fingerprints of each person. When a malpractice occurs, "Already voted" message will be displayed. The Arduino IDE is used for programming the board and cloud is used to display ballot card and to store the result. System provides an alert on malpractice and only an authorized voter can cast the vote. This project safeguards the citizen's right to vote and guarantee fair election.*

1. INTRODUCTION

Elections play a crucial role in a democratic country like India, ensuring that citizens can exercise their right to vote and choose their representatives fairly. Traditional voting methods using ballot papers were time-consuming, prone to errors, and vulnerable to fraudulent activities such as multiple voting and unauthorized access. To overcome these challenges, Electronic Voting Machines (EVMs) were introduced, significantly improving the efficiency and reliability of the election process. This project focuses on developing an advanced EVM using the Raspberry Pi Zero 2W, incorporating biometric authentication to enhance security and prevent unauthorized voting. The system consists of a fingerprint module for voter verification, nines witches for casting votes, an LCD display for showing voting-related information, and a buzzer to alert unauthorized access attempts. Initially, voter fingerprints are enrolled and stored in the system. During the voting process, a voter places their finger on the fingerprint module, which verifies their identity against the stored database. If authentication is successful, the voter can cast their vote by pressing one of the nine switches corresponding to different political parties. If an unregistered person attempts to vote, the system denies access and triggers a buzzer alert. Once the voting process is complete, the administrator can access and display the election results by scanning their fingerprint. The total votes for each party are calculated and displayed on the LCD screen. Additionally, the system provides an option to reset stored data if required. By integrating biometric authentication, this EVM ensures a secure, transparent, and fraud-resistant voting process, making elections more reliable and efficient.

2. EMBEDDED SYSTEMS

An embedded system is a computer system designed to perform one or a few dedicated functions often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts. By contrast, a general purpose computer, such as a personal computer (PC), is designed to be flexible and to meet a wide range of end-user needs. Embedded systems control many devices in common use today. Embedded systems are controlled by one or more main processing cores that are typically either microcontrollers or digital signal processors (DSP). The key characteristic, however, is being dedicated to handle a particular task,

which may require very powerful processors. For example, air traffic control systems may usefully be viewed as embedded, even though they involve mainframe computers and dedicated regional and national networks between airports and radar sites. (Each radar probably includes one or more embedded systems of its own.) Since the embedded system is dedicated to specific tasks, design engineers can optimize it to reduce the size and cost of the product and increase the reliability and performance. Some embedded systems are mass-produced, benefiting from economies of scale. Physically embedded systems range from portable devices such as digital watchesandMP3players, 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 a strictly definable term, as most systems have some element of extensibility or programmability. For example, handheld computers share some elements with embedded systems such as the operating systems and microprocessors which power them, but they allow different applications to be loaded and peripherals to be connected. Moreover, even systems which don't expose programmability as a primary feature generally need to support software updates. On a continuum from "general purpose" to "embedded", large application systems will have subcomponents at most points even if the system as a whole is "designed to perform one or a few dedicated functions", and is thus appropriate to call "embedded". A modern example of embedded system is shown in figure1.

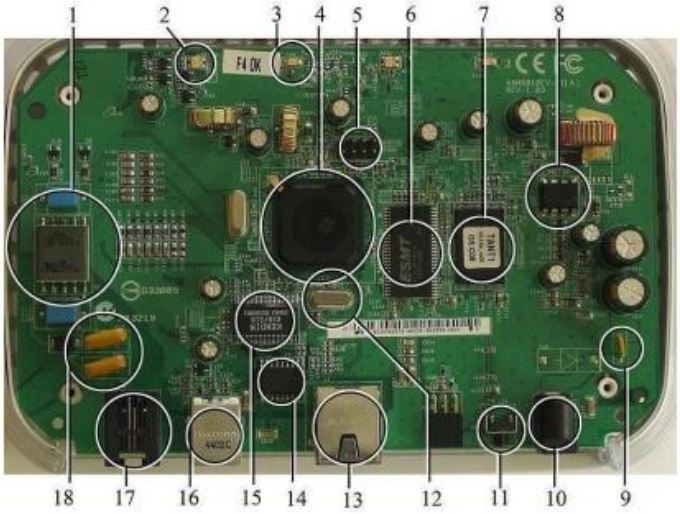


FIGURE 1. A modern example of embedded system

Labeled parts include microprocessor (4), RAM (6), flash memory (7). Embedded systems programming is not like normal PC programming. In many ways, programming for an embedded system is like programming PC 15 years ago. The hardware for the system is usually chosen to make the device as cheap as possible. Spending an extra dollar, a unit in order to make things easier to program can cost millions. Hiring a programmer for an extra month is cheap in comparison. This means the programmer must make do with slow processors and low memory, while at the same time battling a need for efficiency not seen in most PC applications. Below is a list of issues specific to the embedded field.

Need for Embedded Systems: The potential applications of embedded systems are virtually endless; as new products constantly emerge that incorporate embedded computers in innovative ways. In recent years, the cost of hardware like microprocessors, microcontrollers, and FPGA chips has significantly decreased. As a result, when designing a new control system, it is often more practical and cost-effective to purchase a standard chip and develop custom software for it, rather than creating a specialized chip for specific tasks, which can be time-consuming and expensive. Many embedded systems also come equipped with robust libraries, making software development relatively simple. From an implementation perspective, embedded systems differ from general-purpose computers in that they often need to deliver real-time responses. What sets embedded systems apart is their high reliability and the ease with which they can be debugged.

Embedded systems are specialized computing systems designed to perform dedicated functions within larger mechanical or electrical systems. These systems are typically built around microcontrollers or microprocessors and are optimized for efficiency, reliability, and real-time operation. Embedded systems come in various forms,

such as standalone systems like microwave ovens and air conditioners, real-time systems used in mission-critical applications (e.g., automotive control or industrial automation), and networked communication systems like smart door locks and webcams. Software architectures for embedded systems range from simple control loops to complex multitasking kernels, including cooperative multitasking, primitive multitasking, and microkernel-based designs. The choice of architecture depends on the application's complexity, timing requirements, and available system resources.

FIGURE 2. Network communication embedded systems

Embedded systems are extensively utilized across multiple fields due to their effectiveness and specialization in handling specific tasks. In consumer electronics, they are integrated into everyday items such as microwave ovens, TV remotes, DVD players, and digital cameras. For office environments, embedded systems support devices like printers, fax machines, and modems, contributing to improved workflow and communication. In industrial settings, they are essential for controlling and monitoring variables like temperature, pressure, and voltage, and are often used to operate machinery or robots in dangerous areas where human presence is limited. Furthermore, embedded systems are vital in computer networking—found in devices like routers and network bridges—and in telecommunications, where they power mobile phones and webcams, enabling efficient communication and data transfer.

3. HARDWARE DESCRIPTION

The main components of this project include a Raspberry Pi 3 processor, adapter, push buttons, LCD, SD card, LED indicators, fingerprint module, and a buzzer, all working together to perform a specific embedded system task. The Raspberry Pi 3, based on the ARM11 processor, is a powerful 32-bit RISC microprocessor core that supports complex embedded applications with high computational demands. Unlike microcontrollers, which integrate all components on a single chip for simpler, task-specific functions, microprocessors like the ARM11 offer greater flexibility, multitasking, and performance with faster clock speeds, extended instruction sets, and external memory and I/O interfacing. The ARM11 architecture, based on enhanced RISC principles, includes advanced features like SIMD media instructions, better pipeline design, cache management, and multiprocessor support, making it suitable for demanding applications such as industrial automation and multimedia processing. It is widely used in mobile devices and embedded systems, as seen in chips like the Broadcom BCM2835 used in the Raspberry Pi, enabling a wide range of high-performance and energy-efficient solutions.

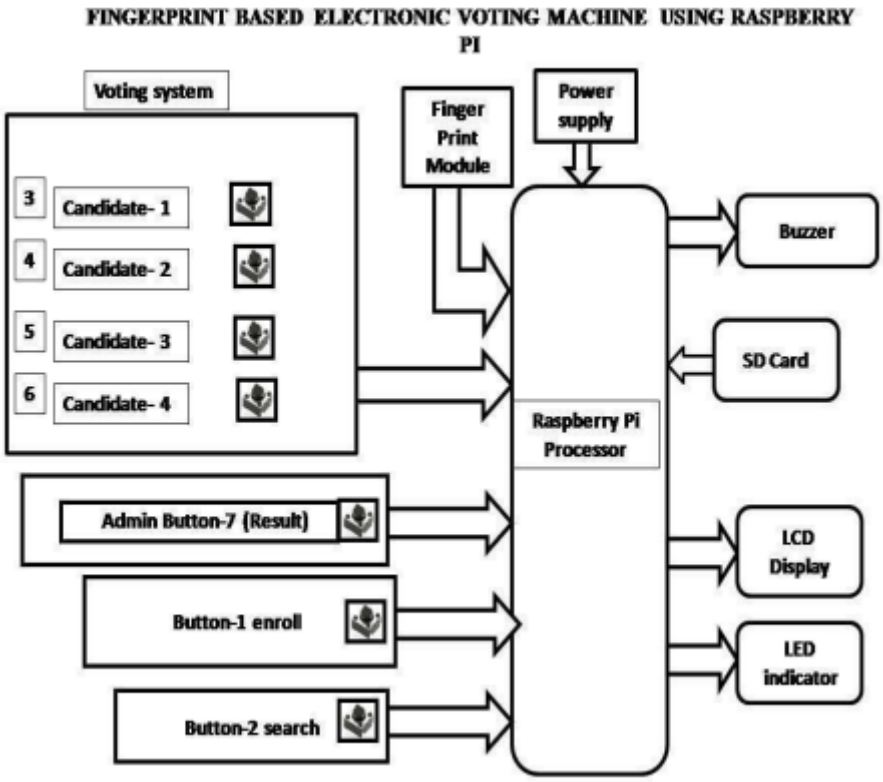


FIGURE 3. Block Diagram of Fingerprint Based Electronic Voting System Using Raspberry Pi

Raspberry Pi Zero 2w:

The Raspberry Pi Zero 2 W comes with built-in WiFi capabilities, supporting both the 2.4GHz and 5GHz frequency bands, along with Bluetooth 5.0. This means it can connect to wireless networks and Bluetooth-enabled devices without the need for any external adapters or additional hardware.

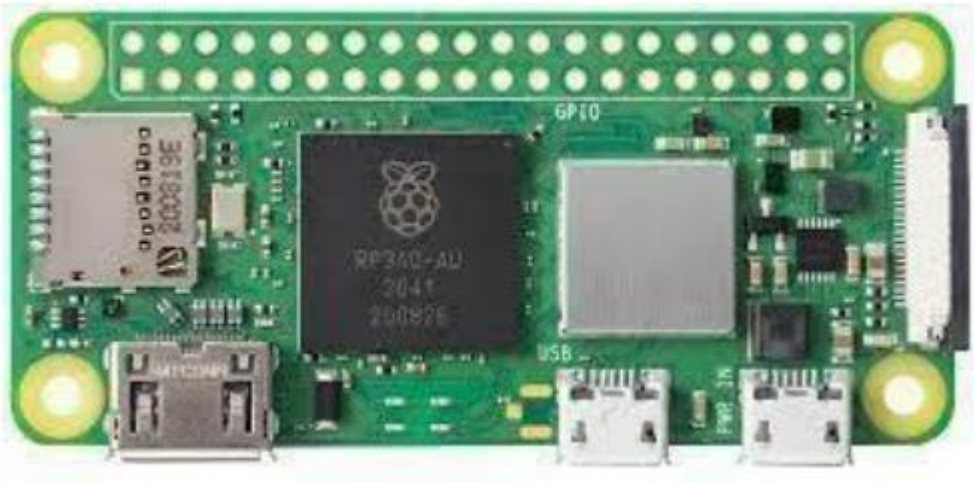


FIGURE 4. Raspberry Pi Zero 2W specification

The Broadcom BCM2710B0 is a quad-core Cortex-A53 (ARMv8) 64-bit System-on-Chip (SoC) operating at 1GHz, serving as the processor for the Raspberry Pi model in use. It is paired with 512MB of LPDDR2 SDRAM, providing efficient performance for lightweight embedded applications. For connectivity, the board supports dual-band 2.4 GHz and 5 GHz IEEE 802.11b/g/n/ac wireless LAN, along with Bluetooth 5.0 and BLE, enabling robust wireless communication. It features a 40-pin GPIO header that is fully backward-compatible with previous Raspberry Pi models, allowing versatile hardware interfacing. Video and audio capabilities include a Micro-

HDMI port supporting up to 1080p60 video output, a MIPI CSI camera connector, and a 3.5mm audio jack. Storage is managed via a microSD card slot used for both operating system booting and data storage. Power is supplied through a 5V DC USB Type-C connector or directly via the GPIO header, with a minimum current requirement of 3A. Compact and lightweight, the board measures just 66mm × 30.5mm × 5mm and weighs 9 grams, making it ideal for space-constrained embedded system designs.

The Samsung 2 Amp 5 Volt Adaptive Fast Charging adapter is a compact and efficient power solution designed primarily for Samsung smartphones, including the Galaxy Note 4 and other micro USB-compatible devices. Utilizing Adaptive Fast Charging technology, it can boost a phone's battery from 0% to 50% in approximately 30 minutes, allowing users to spend less time tethered to an outlet. This adapter supports rapid charging with an output of 2.0A, which is significantly faster than standard 1 Amp or 700mAh chargers. Its detachable USB to Micro USB cable adds flexibility, enabling charging via wall outlets or USB ports on computers and other power sources. The charger also supports file synchronization and transfer between smartphones and computers. Compact and travel-friendly, the charger features short circuit protection, ensuring safe, reliable use. It supports a wide input voltage range (AC 100–240V, 50–60Hz) and is suitable for use in various locations including homes, offices, and vehicles. This charger is compatible with numerous Samsung models and other micro USB devices, offering quick and dependable charging wherever needed.

A Light Emitting Diode (LED) is a semiconductor-based light source widely used as indicator lamps in devices and increasingly adopted in general lighting due to its energy efficiency and longevity. First introduced in 1962, early LEDs emitted low-intensity red light, but advances in technology have enabled the production of LEDs across the entire visible spectrum, as well as ultraviolet and infrared wavelengths, with high brightness levels. LEDs are valued for their compact size, low power consumption, and durability, making them ideal for a broad range of applications from simple indicators to sophisticated lighting systems. Figures 3.4.1 and 3.4.2 illustrate the internal structure and components of an LED, highlighting its functional design and operating principle.

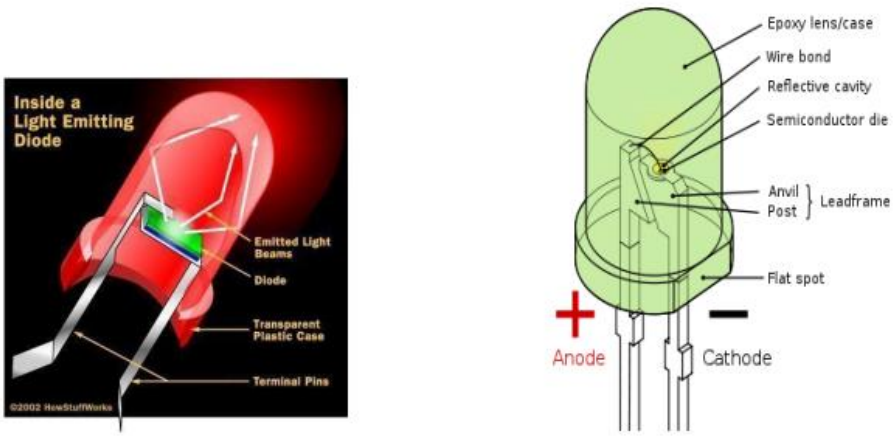


FIGURE 5. Inside a LED and Parts of a LED

The working principle of an LED (Light Emitting Diode) is fundamentally different from that of a traditional incandescent bulb, though its structure is remarkably simple and durable. At its core, the LED is built on a semiconductor diode, and the light it emits depends on the type of semiconductor material used, which determines the color of the emitted light. When the LED is forward-biased—meaning current flows through it—electrons recombine with holes in the diode's active region, releasing energy in the form of photons. This phenomenon is known as electroluminescence. The colour of the emitted light is determined by the energy gap of the semiconductor material. Typically, LEDs are very small in size (usually less than 1 mm^2), and often include optical components to control the light's radiation pattern and improve reflection. LEDs offer many advantages over traditional incandescent bulbs, including significantly lower energy consumption, a much longer operational life, faster switching times, higher durability, and improved reliability. However, they are generally more expensive and require precise current regulation and thermal management. Despite their higher initial cost, LEDs are widely used in automotive lighting, traffic signals, and high-speed data transmission systems, thanks to their compact size, high brightness, and rapid switching capabilities.

Fingerprint Module

The fingerprint scanner, a vital identification device, has its origins in the late 19th century, gaining popularity for its ease of data acquisition and the uniqueness of fingerprints. Its fundamental basis lies in Galton points, identified by Sir Francis Galton, which describe unique fingerprint characteristics. In 1969, the FBI initiated efforts to automate fingerprint recognition, collaborating with the National Institute of Standards and Technology (NIST) to improve scanning, matching, and searching of fingerprints using minutiae-based technology. A prototype using capacitive scanning was introduced in 1975. Modern fingerprint identification systems consist of a sensor for scanning, a processor to analyse data, and software to match the scan against a stored database. Fingerprints are highly individual due to DNA-defined ridge patterns and valley structures on the skin, making them reliable for personal identification.

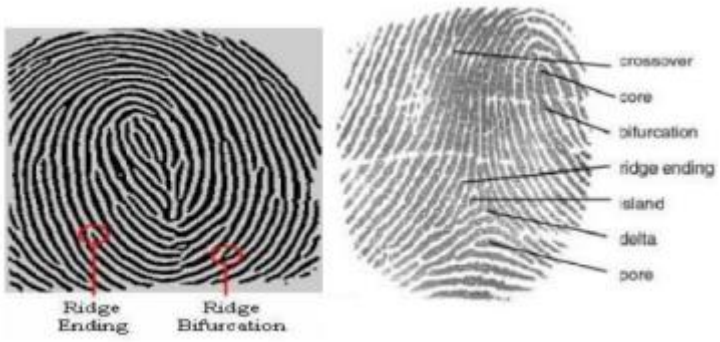


FIGURE 6. Fingerprint

Fingerprint scanners operate primarily through two technologies: optical and capacitive scanning. Optical scanners use a CCD (Charge Coupled Device) to capture a light-based image of the finger by analysing the pattern of ridges and valleys, forming a digital representation. The system checks image quality by evaluating pixel darkness and definition before comparing it with stored data. On the other hand, capacitive scanners use electrical signals to form an image by detecting variations in capacitance caused by the ridges and valleys of the fingerprint. These scanners offer more security and compactness compared to optical types, as they require an actual fingerprint surface to function, making them less vulnerable to spoofing.

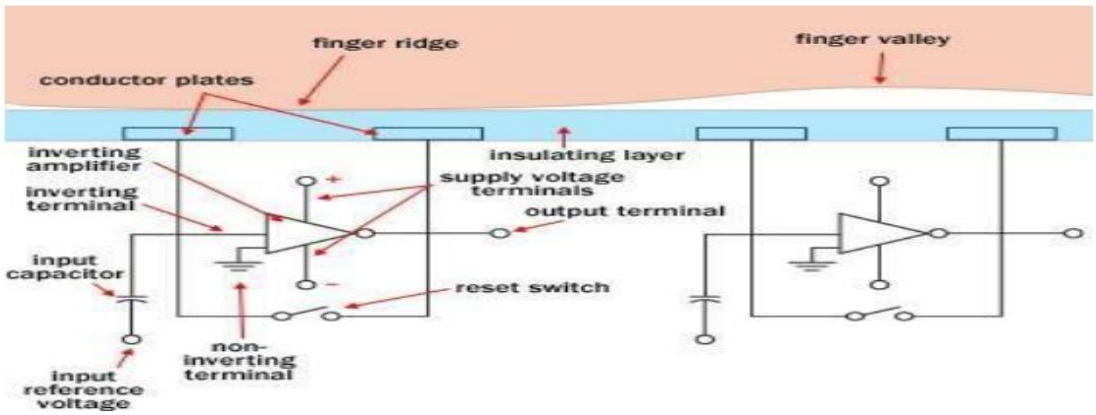


FIGURE 7. Fingerprint Scanner Circuit Diagram

LCD Display: In interfacing an LCD with a microcontroller, three control lines—EN (Enable), RS (Register Select), and RW (Read/Write)—are essential, along with either a 4-bit or 8-bit data bus depending on the chosen mode of operation. Using a 4-bit mode reduces the number of required I/O lines to 7, while 8-bit mode requires 11. The EN line plays a crucial role, signalling the LCD to execute an instruction once the data and control lines are ready. Communication begins with CLREN (clearing EN low), followed by setting data and control lines, then SETB EN (setting EN high), and finally lowering EN again to execute the command. Since the RW line is often tied to write mode to simplify the design, LCD status (like the busy flag at DB7) can't be read back, so precise software delays are inserted to ensure synchronization. The RS line differentiates between instructions and data,

and a 10k potentiometer is used to control LCD contrast. Proper timing and handling of the EN line is essential for reliable LCD communication, especially with different microcontroller speeds and crystal frequencies.

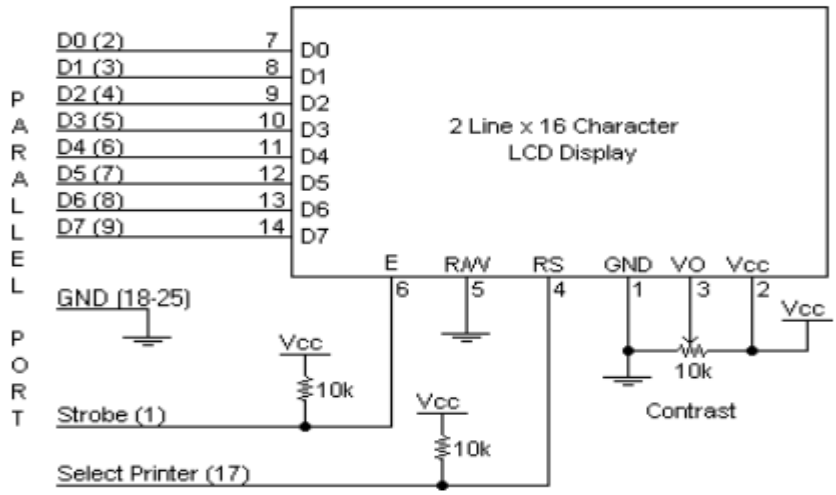


FIGURE 8. LCD Connection Diagram

Buzzer: A piezoelectric buzzer generates sound using a piezoelectric diaphragm, which consists of a piezoelectric ceramic plate bonded to a metal plate (such as brass or stainless steel). When DC voltage is applied across the electrodes of the diaphragm, it experiences mechanical distortion due to the piezoelectric effect, causing the diaphragm to bend. Applying an AC voltage causes this bending to occur repeatedly, generating sound waves in the air. For interfacing, a standard transistor driver circuit is typically used. If a separate power supply is used for the buzzer, the ground lines must be shared to ensure proper operation. Piezo buzzers differ from piezo sounders in that buzzers usually emit a single fixed tone and draw more current, while piezo sounders can produce multiple tones. When using self-driven piezo buzzers, special care must be taken to ensure proper switching, maintain recommended voltage levels (3V–20V), and avoid series resistors, as they may interfere with oscillation. Additionally, the sound-emitting hole should remain unobstructed, and a clear space of at least 15mm should be maintained in front of the buzzer for effective sound transmission.

FIGURE 9. Buzzer

A push-button, also known as a control switch, is a simple switch mechanism used to control machines or processes. Typically made of hard materials like plastic or metal, push-buttons are designed to be easily pressed by a human finger or hand. They are commonly spring-loaded to return to their original position after being pressed. Push-buttons are widely used in everyday devices such as calculators, telephones, and kitchen appliances, as well as in industrial and commercial settings. In industrial use, they are often color-coded for safety—green for start and red for stop, with emergency stop buttons often having a large "mushroom" head for visibility and accessibility. These buttons can include integrated pilot lights to give users visual feedback when a process is initiated. In more complex systems, push-buttons may trigger a relay or be part of load control switches in smart grids, allowing utilities to manage energy consumption during peak times. These load control switches can automatically reset and are designed to minimize disruptions to appliance functions.

4. SOFTWARE DESCRIPTION

• Kernel - Kernel is the core part of Linux. It is responsible for all major activities of this operating system. It is consists of various modules and it interacts directly with the underlying hardware. Kernel provides the required abstraction to hide low level hardware details to system or application programs.

• System Library - System libraries are special functions or programs using which application programs or system utilities accesses Kernel's features. These libraries implements most of the functionalities of the operating system and do not requires kernel module's code access rights.

• System Utility –System Utility programs are responsible to do specialized, individual level tasks.

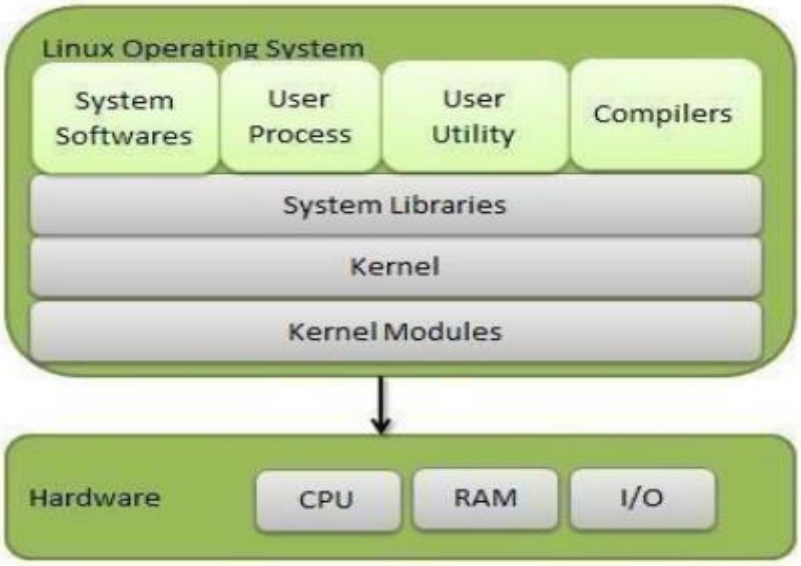


FIGURE 10. Kernel Mode vs User Mode

Kernel component code executes in a special privileged mode called kernel mode with full access to all resources of the computer. This code represents a single process, executes in single address space and do not require any context switch and hence is very efficient and fast. Kernel runs each process and provides system services to processes, provides protected access to hardware's to processes. Support code which is not required to run in kernel mode is in System Library. User programs and other system programs work in User Mode which has no access to system hardware's and kernel code. User programs / utilities use system libraries to access Kernel functions to get system's low level tasks.

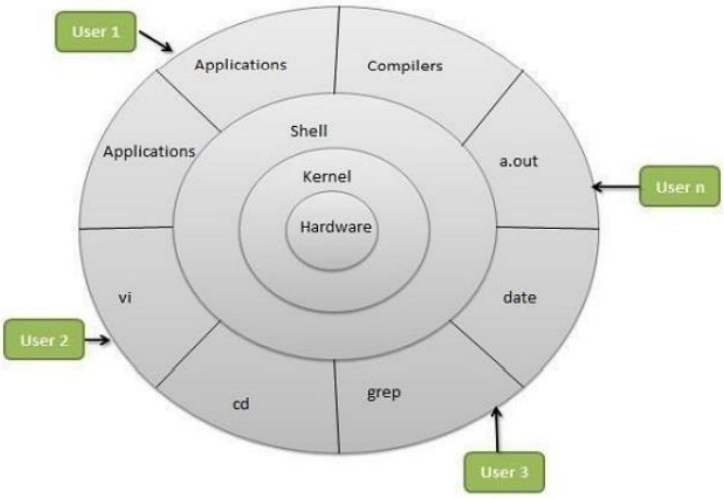


FIGURE 11. Kernel System

Linux System Architecture consists following layers:

• Hardware layer-Hardware consists of all peripheral devices (RAM/HDD/CPU etc.). • Kernel - Core component of Operating System, interacts directly with hardware, provides low level services to upper layer components. • Shell- An interface to kernel, hiding complexity of kernel's functions from users. Takes commands from user and executes kernel's functions. • Utilities – Utility programs giving user most of the functionalities of an operating systems.

Today, Linux has made significant strides in the desktop market, with developers focusing on networking and services, while office applications were the final barrier to overcome. As a result, Linux now offers alternatives to Microsoft Office with compatible applications like word processors, spreadsheets, and presentations. On the server side, Linux is renowned for its stability and reliability, supporting services for major companies like Amazon and the US Post Office, as well as being used extensively by Internet providers for firewall, proxy, and web servers. Additionally, Linux powers clusters for large-scale tasks such as movie production (e.g., "Titanic" and "Shrek") and internet searches. Beyond workstations and servers, Linux runs on a wide range of hardware, from PDAs and mobiles to embedded applications and even experimental wristwatches, making it the only operating system covering such a vast spectrum of devices.

5. RESULT AND DISCUSSION

The paper “Finger Print Based Electronic Voting System Using Raspberry Pi” is mainly intended to develop 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. It allows only registered persons to cast the vote. When an unknown person puts his finger to cast his vote, access will be denied and then the buzzer gives sound alert. If we want to erase the data, we need to press enroll and search buttons simultaneously.

The Fingerprint-Based Electronic Voting System using Raspberry Pi offers several key advantages. It is a tamper-free electronic voting machine (EVM) that ensures a secure and transparent election process. The system is easy to use, allowing voters to cast their votes with fingerprint authentication, ensuring that only registered and authenticated individuals can vote, thereby enhancing security compared to traditional voting equipment. The design is both efficient and cost-effective, with low power consumption, making it suitable for wide deployment. However, the system does come with a notable disadvantage—interfacing the fingerprint module with the Raspberry Pi processor can be sensitive and may require careful handling and configuration. In terms of applications, this system can be practically implemented in real-time voting scenarios such as college elections, corporate office decisions, and government election zones, where secure and reliable voting is essential.

6. CONCLUSION

Integrating features of all the hardware components used have been developed in it. Presence of every module has been reasoned out and placed carefully, thus contributing to the best working of the unit. Secondly, using highly advanced IC’s with the help of growing technology, the project has been successfully implemented. Thus the project has been successfully designed and tested.

Future Scope: By adding MATLAB and USB camera; whenever any unauthorized person cast the vote, the USB Camera takes image of the person and sends email to the predefined mail id. Using USB to TTL we can send the user unique ID to the PC. The voter details a long with the image can be viewed in the PC by using MATLAB. This project can be extended by using finger vein module which can make a difference between a finger which is dead and the finger that is alive.

REFERENCES

[1]. Ch. Srilatha et al. “Fingerprint based Biometric Smart Electronic Voting Machine using IoT and Advanced Interdisciplinary Approaches”, E3S Web of Conferences 507, 01037 (2024).

[2]. Senthilkumar Meyyappan, A. Bharath Naik, A. Uma Sai and Ch. Keerthi, "Improving Weather Forecasting Accuracy Using Machine Learning", *Journal on Electronic and Automation Engineering,* Vol. 2(4), December 2023, pp. 9-18.

[3]. Senthilkumar Meyyappan and N. Selvamuthukumaran, "Network Selection in Heterogeneous Wireless Systems using GRA Method", *Journal on Electronic and Automation Engineering*, Vol. 4(1), March 2025, pp. 127-132.

[4]. Khadija Hasta et al. "Fingerprint Based Secured Voting", International Conference on Advances in Computing, Communication and Control (ICAC3), Dec. 2019.

[5]. M. Senthil Kumar and M. Gopinath, "An Efficient Polynomial Pool-Based Scheme for Distributed Heterogeneous WSNs", *International Journal of Modern Engineering Research (IJMER)*. (Vol.3, Issue 6, Nov-Dec.2013, PP 3328-3335, ISSN: 2249-6645).

[6]. R. Kathiresh, V.M. Ramprasath and M. Senthil Kumar, *"A Systematic Approach for Design of Compressed Test Data in SOC"*, CiiT International Journal of Software Engineering and Technology. (Vol.4, No.4, Issue: April 2012, Print: ISSN 0974 – 9748 & Online: ISSN 0974 – 9632).

[7]. M. Senthil Kumar and L. Praveen, "An Assuring Approach for Tree-Based Routing Topology in WSNs", *International Journal of Emerging Trends in Engineering and Development (IJETED).* (Issue 3, Vol.6, November 2013, ISSN: 2249 – 6149).

[8]. Senthilkumar Meyyappan, G. Lava Kumar, G. Niharika and G. Chakradhar, "Cellular Network Signal Strength Analyser", *Journal on Electronic and Automation Engineering*, Vol. 4(1), March 2025, pp. 165-174.

[9]. R. Kathiresh, P. Kalidass and M. Senthil Kumar, *"A Study of Energy Efficient Embedded Processor and its Reuse"*, International Journal of Modern Engineering Research (IJMER). (Vol.2, Issue 3, May-June 2012, PP 830-833, ISSN: 2249-6645).

[10]. Senthilkumar Meyyappan, K. Susmitha, K. Vaishnavi and M. Sai Rao, "Condition Based Monitoring and Maintenance System for Underground Metro Stations", *Journal on Electronic and Automation Engineering*, Vol. 4(1), March 2025, pp. 175-182.

[11]. C. Sridhathan, M. Senthil Kumar and G. Rajesh Krishna, *"Smart and Secure Railway Transport System",* Journal of Computing Technologies (JCT). (Vol.7, Issue 8, August 2018, ISSN: 2278 – 3814).

[12]. C.I. Vimalarani and M. Senthil Kumar, "Energy Efficient PCP Protocol for k-Coverage in Sensor Networks", *IEEE International Conference on Computational Intelligence and Computing Research, IEEE Proceedings, 2010*.

[13]. M. Kavitha, T. Maheshwaran and M. Senthil Kumar, "Secure Routing in MANETs with Key Management", *International Journal on Engineering Technology and Sciences (IJETS).* (Vol.1, Issue 6, October 2014, ISSN (P): 2349 – 3968, ISSN (O): 2349 - 3976).

[14]. M. Senthil Kumar, "Energy Efficient Techniques for Transmission of Data in Wireless Sensor Networks", *Journal of Computing Technologies (JCT)*. (Vol.5, Issue 2, February 2016, ISSN: 2278 – 3814).

[15]. M. Senthil Kumar and Ashish Chaturvedi, "Energy-Efficient Coverage and Prolongs for Network Lifetime of WSN using MCP*", European Journal of Scientific Research (EJSR).* (Vol.95, No.2, January 2013, ISSN: 1450 – 216X / 1450 – 202X).

[16]. K. Arutselvan, C. Sridhathan and M. Senthil Kumar *"Unlocking Mobile Devices using Improved Face Recognition and Eye Blinking Technique",* International Journal of Applied Engineering Research (IJAER). (Vol.13, No.24, 2018, PP 16907-16909, ISSN: 0973-4562).

[17]. M. Senthil Kumar and C. Sridhathan, "Impact of Mobility on the Routine of Enhanced – DSDV Protocol in Mobile Ad-hoc Networks", *International Journal of Applied Engineering Research (IJAER)*. (Vol.13, No.14, 2018, PP 11674-11679, ISSN: 0973-4562).

[18]. M. Kavitha, T. Maheshwaran and M. Senthil Kumar, "Ensure Data Transmission in Mobile Ad-Hoc Networks", *International Journal on Engineering Technology and Sciences (IJETS)*. (Vol.2, Issue 4, April 2015, ISSN (P): 2349 – 3968, ISSN (O): 2349 - 3976).

[19]. M. Senthil Kumar and Ashish Chaturvedi, "A Novel Enhanced Coverage Optimization Algorithm for Effectively Solving Energy Optimization Problem in WSN", *Research Journal of Applied Sciences, Engineering and Technology (RJASET).* (Issue 4, Vol.7, January 2014, ISSN: 2040 – 7459 & e-ISSN: 2040 – 7467).

[20]. Senthilkumar Meyyappan, Kalyan Kasturi, G. Vijaya Lakshmi, J. Srinija Reddy and K. Grace Sampoorna, "Improvement of LEACH Protocol for Enhancing Features of WSN", *Journal on Electronic and Automation Engineering*, Vol. 2(4), December 2023, pp. 19-26.