IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 03, March 2026 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1303.43

Secure Electronic Voting System Using IoT and Biometric

V.Gowthaman
Assistant Professor, Department of Electronics and Communication Engineering,
Sengunthar Engineering College (Autonomous), Tiruchengode, India
vgowthaman.ece@scteng.co.in
https://orcid.org/0009-0005-5119-1681
D.Muthukumar ,M.Nandhakumar,R.Vishal
UG Scholars, Department of Electronics and Communication Engineering,
Sengunthar Engineering College (Autonomous), Tiruchengode, India

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.13/Issue03/AEMR26.MRAE10122
Research Article | Open Access | Double-Blind Peer-Reviewed |Article ID:IJIRAE/RS/Vol.13/Issue03/AEMR26.MRAE10122
Received:22,February 2026, Revised: 01, March 2026, Accepted: 16,March 2026,Published Online: 25, March 2026.
https://www.ijirae.com/volumes/Vol13/iss-03/43.AEMR26.MRAE10122.pdf
Article Citation: Gowthaman,Muthukumar,Nandhakumar,Vishal(2026),Secure Electronic Voting System Using IoT and Biometric, IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 13, Issue 03 of 2026 pages 339-354 **Doi:>** https://doi.org/10.26562/ijirae.2026.v1303.43
BibTeX Key: Gowthaman@2026 Secure
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2026.v1303.43 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: In recent years, electoral processes across various regions have faced significant challenges related to voter fraud, identity theft, and low trust in the security and transparency of traditional voting systems. Manual verification methods are often time-consuming, prone to human error, and vulnerable to manipulation. This project proposes a secure and efficient voting system that integrates RFID (Radio Frequency Identification) and face recognition technologies to authenticate voter identity and ensure fair voting practices. The system is designed to eliminate common issues such as impersonation, multiple voting, and the use of fake identification by combining contactless RFID verification with advanced facial biometrics. Each voter is issued a unique RFID card linked to their personal and facial data stored in a secure database. Upon arrival at a polling station, the voter presents their RFID card, and their identity is verified in real-time using facial recognition. Only upon successful dual authentication is the voter allowed to cast their vote. This approach enhances the security, accuracy, and speed of the voting process while maintaining privacy and user-friendliness. By leveraging modern identification technologies, the system aims to restore public trust in democratic processes and offer a scalable solution for local, regional, and national elections.

Keywords: RFID, face recognition, secure voting system, biometric authentication, voter verification, electoral fraud prevention, smart elections.

I. INTRODUCTION

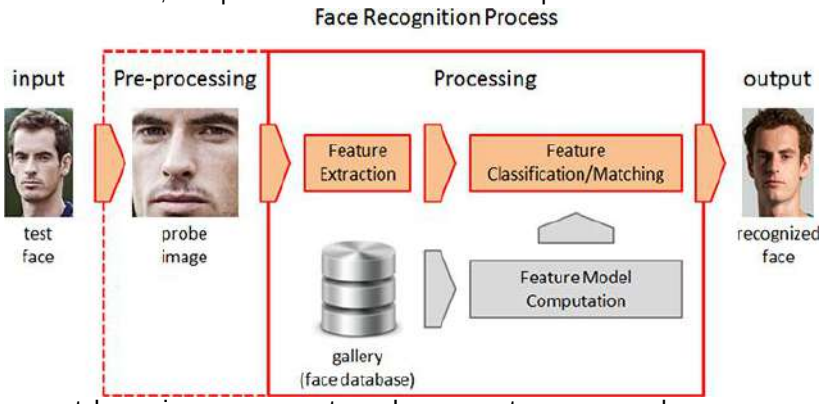
Voting is commonly related to politics and is finished with often exploitation and manual approach where voters stand to vote for his or her decisions. Manual voting may lead to malpractices sometimes.so there is a need to implement online voting system. This is for expand the technology from manual voting system to digital voting system. Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process. Electronic voting has been deployed in many different types of election throughout the world for several decades. Elections form a major part of any democratic society to elect its new government. In earlier times, paper-based elections were conducted. In that, voters cast their votes on the ballot paper and then drop that paper in sealed boxes provided by the election department. When the elections end, the secret ballots are opened and manually counted to proclaim results. The traditional or paper based polling method served to increase people's confidence in the selection by majority voting. It has helped make the democratic process and the electoral system worthwhile for electing constituencies and governments more democratized. There are 167 nations with democracy in 2018, out of approximately 200, which are either wholly flawed or hybrid [5,6]. The secret voting model has been used to enhance trust in democratic systems since the beginning of the voting system. It is essential to ensure that assurance in voting does not diminish. A recent study revealed that the traditional voting process was not wholly hygienic, posing several questions, including fairness, equality, and people's will, was not adequately [7] quantified and understood in the form of government [2,8]. But in this process sometime there can be manually error or cheating to declare the results. Also, there is lot of wastage of paper and manpower.

E- VOTING MACHINE

The Indian government installed direct record electronics - DRE voting system which are popularly known as E-voting machines – EVMs. The ideation in this work is to redesign electronics voting system to make the system more efficient and reliable. However, the manipulation of voting results still exists. The unreliable nature of the voting system and delays in results of the existing system is the prime motivation to study for alternative and more secure methods of online voting. Also, the COVID-19 Pandemic have accelerated the use of technologies which includes online shopping, digital payments, tele health, AI, Remote work, Distance education and online internet. So online voting also seems imminent. The election processes are primarily held through ballot papers, with eligible voters having to select their candidate/party by marking on the ballot paper. Some countries, like India, utilize a slightly more technological approach to elections, by using Electronic Voting Machines (EVMs), which allow voters to cast their vote by clicking on a button representing the party/candidate of their choice. The election processes currently in place involve a trusted third party, like the election commission or election administration, required to manually tally the votes from ballot papers or EVMs, and aggregate the vote counts from various geographical regions in the country to calculate the final result. Now, since the entire election process is offline, there is a greater chance of malpractice and unfair means of elections which is a threat to our democracy. However, the existing voting system isn't completely fool proof and reliable. There are a lot of concerns involving tampering of votes, manipulation of results, fake voters, and anonymity of the voter, transparency and security. Also, the voters need to go to distributed places like polling booths and stand in a long queue to cast their vote, because of these reasons most of the people misses their chance of voting. The voter who is not eligible can also cast its vote by fake means which may leads to many problems. This motivates us to build a voting system which is online and can address few of the afore-mentioned issues.

FACE VOTING SYSTEM

In recent years, low-resolution face recognition has attracted a wide range of attention due to its potential for civilian applications. Compared with face, fingerprint, and iris based biometrics systems, low-resolution face based biometrics system has several special advantages such as stable and rich line features, small distortion and easy self-positioning. In addition, it can achieve high accurate recognition rate (ARR) and low equal error rate (EER) with decent time efficiency. Many effective face recognition methods have been proposed, which can be roughly divided into categories such as texture-based, line-based, subspace learning-based, correlation filter-based, local descriptor-based, and orientation coding-based. It is well known that palm lines, including principal lines and wrinkles, are essential features in low resolution face images. On the one hand, face contains strong direction feature along with palm lines. On the other hand, direction feature is insensitive to illumination change, which frequently bothers face recognition algorithms. For these reasons, direction information has been popularly encoded for face recognition. In the following, for a face image, we call a matrix of direction values at all pixels as a direction representation (DR) of the particular direction used. Many previous approaches use DRs for face recognition. Face identification is an important personal identification technology and it has attracted much attention. The face contains not only principle curves and wrinkles but also rich texture and miniscule points, so the face identification is able to achieve a high accuracy because of available rich information in face . Various face identification methods, such as coding based methods and principle curve methods have been proposed in past decades. In addition to these methods, subspace based methods can also perform well for face identification.



For the security purpose we take various measures to make our system more and more secure that no one can break the security and integrity of the system maintain. By using the password system in which user need to enter the ID name and their password. But in password system, there is always a good chance of forget password because now a day's complexity of password is make so high that no one easily guess other password but this cause another problem that person easily forget their password .If someone get anyone password by any mean then also their id can be used by other person and their data may easily access by other person. Secondly by using identity card method in which ID card is become the identity of person. In this anyone can use their ID card even without their .Biometric authentication can be done by using physiological characteristic which signifies human body parts for authentication like fingers, iris ,face etc

FACE TECHNOLOGY

Biometrics has been an emerging field of research in the recent years and is devoted to identification of individuals using physical traits, such as those based on iris or retinal scanning, face recognition, fingerprints, or voices. As unauthorized users are not able to display the same unique physical properties to have a positive authentication, reliability will be ensured.

Face is preferred compared to other methods such as fingerprint or iris because it is distinctive, easily captured by low resolution devices as well as contains additional features such as principal lines. The input devices are expensive and the method is intrusive as people might fear of adverse effects on their Fingers. Fingerprint identification requires high resolution capturing devices and may not be suitable for all as some may be finger deficient. Face is therefore suitable for everyone and it is also non-intrusive as it does not require any personal information of the user. Face images are captured by acquisition module and are fed into recognition module for authentication. Compared with face recognition face is hardly affected by age and accessories. Compared with fingerprint recognition face images contain more information and needs only low resolution image capturing devices which reduces the cost of the system. Compared with iris recognition the face images can be captured without intrusiveness as people might fear of adverse effects on their Fingers and cost effective. Hence it has become an important and rapidly developing biometrics technology over the last decade. Limited work has been reported on face identification and verification, despite the importance of face features. The system functions by projecting face images onto a feature space that spans the significant variations among known images.

II. LITERATURE SURVEY

2.1 A Timed-Release E-Voting Scheme Based on Paillier Homomorphic Encryption

Author: Ke Yuan; Peng Sang/Year: 2024

E-Voting is widely used in many social, economic, political and cultural fields for its convenience, efficiency and greenness, but how to guarantee the fairness of e-voting and the controllability of human intervention needs further in-depth research and exploration. Although the introduction of homomorphic encryption algorithm solves the problem of ballot privacy calculation, and most of these schemes solve the problem of private key confidentiality by using or overlaying multiple different methods of saving private keys, its security will be questioned as long as there is a possibility of human intervention in the saving process. To solve this problem, we propose a timed-release e-voting scheme based on Paillier homomorphic encryption. We analyze the semantic security of the ballot formally by defining the security game, and realize the legitimacy check of the ballot ciphertext through the idea of partial knowledge proof. Property analysis shows that this scheme satisfies the basic properties of the security requirements of the e-voting scheme. Performance analysis shows that this scheme is feasible to implement in practical voting..

2.2 Blockchain Democracy: A Case for Constituency-Centric E-Voting on Private Ethereum Networks

Author: Shraddha Vasant Prasad/ Year: 2024

Blockchain-based Electronic voting (e-voting) systems hold great promise for enhancing the efficiency and safeguarding the integrity of traditional electoral processes. The adoption of blockchain technology, a decentralized ledger system, has become essential to modern e-voting systems, fortifying the security of the electoral process. This research, introduces a practical perspective by fragmenting the blockchain into smaller, constituency-based blockchains, departing from the conventional monolithic single blockchain structure. This approach effectively tackles the formidable challenges associated with elections involving numerous constituencies and a vast electorate. The proposed constituency-based blockchain architecture significantly enhances the adaptability and performance of blockchain technology, enabling it to efficiently manage large voter populations in any country by offering practical recommendations for large scale elections.

2.3 ECC-EXONUM-eVOTING: A Novel Signature-Based e-Voting Scheme Using Blockchain and Zero Knowledge Property Author: Suman Majumder; Sangram Ray/Year: 2023

Traditional voting systems mainly comprise of paper polling, electronic ballot system (EVM), mechanical devices, etc., and demand the physical presence of the voters. In the new age of digitization, the electronic voting system has come up with a unique facility to cast votes from any discreet place. However, the e-voting system has to face several challenges regarding security and privacy. To overcome such obstructions, blockchain is introduced in e-voting applications that preserve anonymity, security, and consistency of voter-related information with the help of Merkle tree and hash digest. Hence, any discrepancy can immediately be detected whenever the hash values of the respective block have been modified and consequently, the whole block is discarded. In this research, a novel e-voting scheme is proposed following the decentralized service-oriented architecture of Exonum private blockchain, hybrid consensus algorithm, and Elliptic Curve Diffie-Helmen (ECDH) protocol to agree upon a secure session key among different participants. Moreover, the proposed scheme (ECC-EXONUM-eVOTING) employs a zero-knowledge protocol and is customized to work over idemix technologies with a blind signature scheme. Numerous well-known cryptographic attacks are analyzed formally using the probabilistic random oracle model and informally for validating the security strength of ECC-EXONUM-eVOTING. As a result, it is found that the proposed scheme is well-defended against all potential security concerns. Furthermore, the scheme is simulated using both Automated Validation of Internet Security Protocols and Applications (AVISPA) and Scyther tools to demonstrate the proposed scheme is not prone to any security attacks. Finally, it is concluded that the proposed scheme is well-suited for secure e-voting applications.

2.4 Securing E-Voting using Hyperledger Fabric: A Permissioned Blockchain Approach

Author: Chirag Jain; Luv Gupta/ Year: 2023

Democracy, a system of governance founded on the principle of citizen representation, has become prevalent worldwide. Elections are crucial components of democratic systems, and it is essential to guarantee transparent, secure, and impartial election processes to maintain citizens' trust in the government. However, the lack of transparency and security in democratic elections has raised concerns about their legitimacy and fairness. Creating a secure e-voting system that provides fairness, anonymity, transparency, and flexibility has been a significant challenge, despite the increasing adoption of technology worldwide. Electronic Voting Machines (EVMs) offer time and effort-saving benefits compared to traditional paper ballots but are susceptible to challenges that compromise the integrity of the electoral process.

To address these challenges, we have proposed a Blockchain based E-voting system. This system provides a secure, decentralized platform where votes are recorded on an immutable ledger. It enables real-time vote counting, overcoming the time-consuming and error-prone nature of traditional methods. The proposed approach involves using Hyperledger Fabric and Chaincode to develop a scalable, maintainable, and cost-effective e-voting system within a customized private Blockchain network. This system adheres to the principles of Zero Knowledge Proof, ensuring accurate vote accounting and safeguarding the credibility and legitimacy of democratic elections.

2.5 E-Voting Blockchain: Enhancing The Security And Transparency of Digital Voting

Author: Siti Fatimah Az Zahra Binti Mohd Nizam/Year: 2023

Voting is synonymous with general elections especially for countries with democratic system. In an effort to slow down the spread of Covid-19, there is a significant rise in digitalization, and this includes voting. However, concerns regarding security and integrity of the entire system have been raised. The implementation of blockchain in voting is believed can help alleviate the issues raised since blockchain are immutable and decentralized. The usage of smart contract that stores states and run when certain conditions are met can get rid of the possibility of database manipulation while still maintaining anonymity. Unfortunately, implementing an Ethereum-based blockchain is expensive as each transaction cost can cost up to thousands of US dollar. Hence, this study focuses on developing an E-Voting blockchain based prototype using a local chain platform that performs the same operations as blockchain but uses a fake currency which results in a more feasible and cost-effective result. In this context, the objectives of this study were to design and develop the smart contract that satisfies the voting requirement and lastly; to evaluate the performance and security of the developed smart contract; to test the functionality of this study's prototype. The prototype of this study was developed using a combination of Web 2.0, PHP, MySQL, Express.js and Web 3.0, specifically Ganache, Remix IDE and MetaMask. After the development and integration phases, the prototype was evaluated and validated using unit testing, which tested each function and modules individually before being integrated to ensure full functionality of each module. A total of 20 voters were gathered to test the prototype for the user acceptance testing section of the prototype of this study which shows the viability and usability of the product. E-Voting blockchain based prototype successfully achieved the objectives and solved the problems stated in the proposal. Despite the limitations, there are still...

2.6 SWOT Analysis of E-Voting System in Higher Education Institutions

Author: Aldeniz Rashidov/ Year: 2023

Electronic voting (EV) systems have become integral to modern democratic processes, including those within higher education institutions (HEIs). This study employs a comprehensive SWOT analysis to evaluate the existing EV system in HEI. The analysis elucidates the system's strengths, which encompass its robust security measures, user training initiatives, and innovative features, ensuring a transparent and accessible electoral process. Concurrently, it identifies weaknesses, such as dynamic cybersecurity challenges and potential technological limitations, requiring vigilant monitoring, training, and infrastructure upgrades. The analysis uncovers opportunities for system enhancement. Addressing the identified threats, including cybersecurity vulnerabilities and user resistance, is crucial for ensuring the system's resilience and widespread acceptance. This SWOT analysis serves as a valuable tool for evaluating the EV system in HEIs. It lays the foundation for a strategic plan to enhance the system, improving its security, efficiency, and accessibility. Ultimately, this research contributes to the advancement of transparent and secure electoral processes in HEIs. Blockchain and IoT technologies proved to be a powerful synergy, enhancing the transparency, security, and accessibility of the e-voting system. The system exhibited resilience against potential threats and maintained robust performance throughout the five-year study period. This research underscores the potential transformative impact of Blockchain-enabled E-Voting systems with IoT integration on democratic processes worldwide. It provides a secure and transparent

2.7 A Privacy Protection Method of Blockchain-Based E-Voting Using Homomorphic Encryption and Order-Preserving Encryption Author: Bimeng Tang; Minsheng Tan/ Year: 2023

The blockchain based e-voting system has realized decentralized storage and eliminated the need for third-party trusted institutions to count votes. However, due to the openness of the blockchain, it still has some security issues such as privacy leakage in the voting process. In this paper, we propose a privacy protection method for blockchain-based e-voting system by using homomorphic encryption and order-preserving encryption to avoid privacy leakage. The method transmits the transaction data encrypted by homomorphic encryption through a secure channel and records it on the blockchain, and after the voting is over, the results are encrypted in order and published in ciphertext, which realizes the data confidentiality of the entire voting process and avoids the tracking of malicious users. Experimental results show that the proposed method is feasible in terms of performance and safety.

III.PROPOSED METHOD

The existing voting system in many countries primarily relies on manual or semi-automated processes for voter identification and ballot casting. Typically, voters are required to physically visit polling stations, where their identity is verified using government-issued identification cards such as voter ID, driver's license, or other valid documents. Once verified, voters are either issued paper ballots or directed to electronic voting machines (EVMs) to cast their votes. In traditional paper-based systems, voters mark their choices on a printed ballot, which is then collected in sealed boxes for manual counting. This method, although widely used, is prone to issues such as ballot tampering, human counting errors, and long delays in result declaration. Electronic Voting Machines (EVMs) were introduced in many regions to streamline the process, reduce manual workload, and enhance result accuracy. However, EVMs still require manual voter authentication, typically done by polling officers using identification documents and voter lists. Despite these improvements, the existing systems face several challenges.

These include the risk of voter impersonation, multiple voting, stolen or forged ID cards, and administrative inefficiencies. Additionally, in rural or remote areas, logistical difficulties and lack of staff can compromise the reliability and accessibility of elections. These limitations point to the need for more advanced, automated, and secure voting systems that ensure transparency, accuracy, and trust in the democratic process.

3.1.1 DISADVANTAGES OF EXISTING SYSTEM:

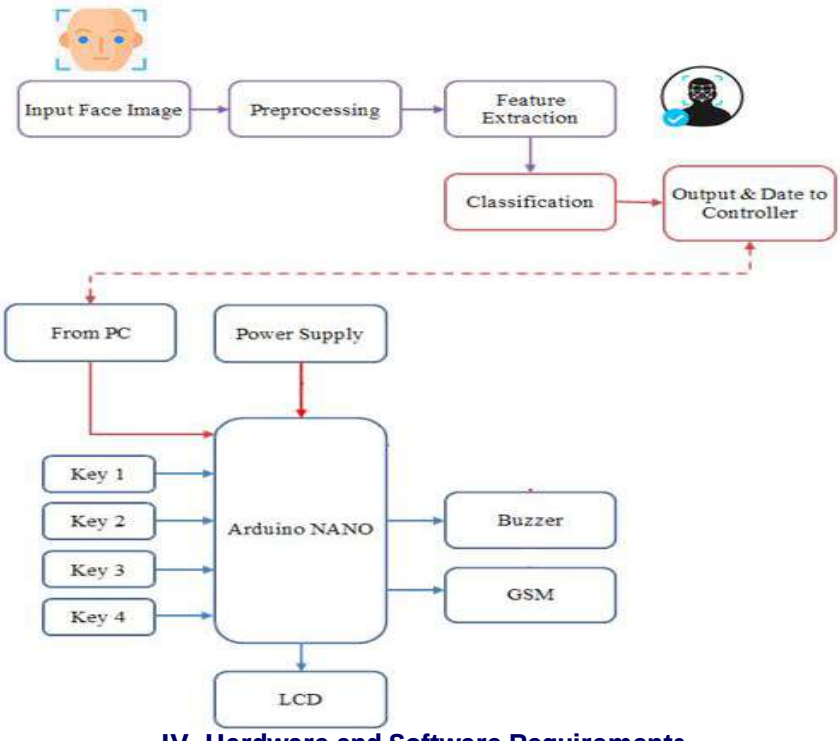
Manual ID verification can be easily manipulated, allowing individuals to vote using fake or stolen IDs, which compromises election integrity. In some cases, voters may find ways to vote more than once, especially if proper electronic tracking is not enforced or if voter rolls are not regularly updated. Manual processes like checking voter lists, issuing ballots, and counting votes can lead to mistakes, affecting the accuracy of election outcomes. Traditional voting and counting methods often result in long lines at polling stations and delays in announcing results. Paper ballots and ID cards can be forged or tampered with, increasing the risk of fraudulent activities. People with disabilities, the elderly, or those in remote areas may find it difficult to reach polling stations or use manual voting methods. Existing systems do not offer real-time verification or data tracking, making it difficult to detect irregularities promptly.

Managing physical polling booths, staff, ballot materials, and security involves significant costs and logistics, especially in large-scale elections.

3.2 PROPOSED SYSTEM

The proposed system is designed to improve the reliability, security, and efficiency of the voting process by combining automated identification and biometric verification methods. Each registered voter is provided with a personalized identification card equipped with a small chip that contains their unique information. This card is linked to a database where their personal and image-based data are securely stored. When a voter arrives at the polling station, they present this card to a scanning device that reads the embedded data. At the same time, a camera captures the voter's live image and compares it to the image stored in the database for verification. This two-step verification process ensures that the individual is eligible to vote and prevents illegal activities such as impersonation or repeat voting. Only after the system confirms the match between the card and the person's image is the individual allowed to proceed and cast their vote through the system interface. All activities are recorded in real time, enabling accurate voter tracking and transparency in the election process. The system is built with multiple modules that handle different tasks such as registration, identity confirmation, vote casting, and data management. It is connected to a central server that allows for live monitoring and quick response to any irregularities. This setup enhances election integrity by ensuring that only authorized individuals participate and that every vote is valid. By reducing human involvement in voter verification and record-keeping, the system minimizes errors, speeds up the process, and builds public trust. It can be scaled and adapted to suit elections of different sizes and environments, offering a forward-looking solution for modern electoral challenges.

BLOCK DIAGRAM OF PROPOSED SYSTEM



IV. Hardware and Software Requirements

4.1 HARDWARE REQUIREMENT

Arduino NANO
RFID
GSM
Input Key

LCD display
Power Supply

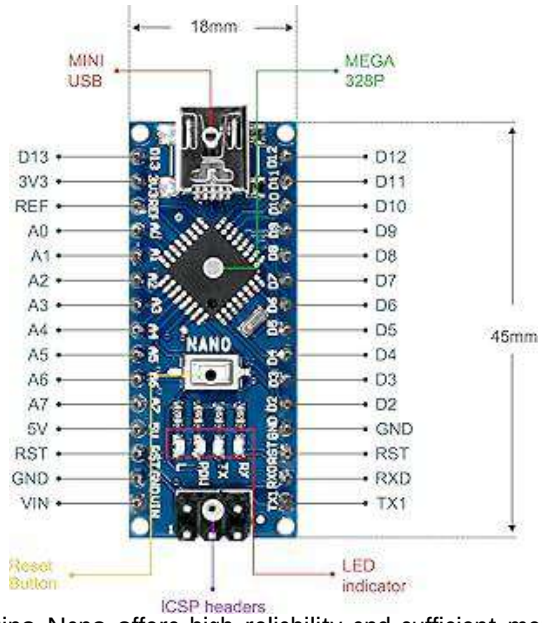
4.2 SOFTWARE REQUIREMENTS

Arduino IDE
Python

4.3 HARDWARE DESCRIPTION

1. Arduino Nano

The Arduino Nano is a compact microcontroller board based on the ATmega328P microchip. Its small size and versatility make it ideal for embedded system applications like smart voting systems. The Nano board features 22 input/output pins, including digital and analog pins, which allow it to interface with a wide range of sensors and modules. It operates at 5V and supports communication protocols such as I2C, SPI, and UART, making it suitable for connecting components like RFID readers, GSM modules, and input keys. One of the key advantages of the Nano is its ease of programming via the Arduino IDE, a user-friendly platform that supports C/C++ programming, allowing developers to quickly prototype and deploy systems. It also includes a mini-USB port for power and data communication with a computer or power source, which is particularly useful in developing interactive systems. In the context of the smart voting system, the Arduino Nano serves as the central processing unit. It collects input from different modules such as the RFID reader, input keypad, and GSM module. For example, when a user scans their card or presses a button, the Nano reads the input signal, processes the data, verifies the user credentials, and then triggers appropriate actions like unlocking the voting interface or sending a confirmation SMS. It also stores temporary data and handles all logical decisions required during the voting process. Furthermore, the Arduino Nano is used to control digital outputs like buzzer alerts or LED indicators, which help guide users through each step of the voting process. Its ability to handle multiple tasks in real time is essential to ensuring smooth system operation.



Despite its compact size, the Arduino Nano offers high reliability and sufficient memory for small-scale applications. It includes 32KB of flash memory, 2KB of SRAM, and 1KB of EEPROM, which can be used to store program code and user data. While not as powerful as larger microcontrollers or processors, the Nano is sufficient for managing the basic logic and communication tasks needed in an RFID and face-recognition-based voting system. Its affordability, ease of integration, and rich development community make it an ideal choice for cost-effective electronic system design. Moreover, the availability of extensive libraries and examples allows developers to customize and scale the system based on specific requirements. In short, the Arduino Nano plays a crucial role in managing the operations, communication, and real-time processing in the proposed secure voting solution.

2. RFID (Radio Frequency Identification)

RFID technology is a wireless communication method that allows data to be transmitted from a tag to a reader using electromagnetic fields. It comprises two main parts: an RFID tag (which is issued to the voter) and an RFID reader (which is installed at the polling station). The tag contains a unique ID and is typically embedded in a card or wearable token. When the voter approaches the reader, the reader sends out a signal that powers the tag and retrieves its unique identification code. This code is then passed on to the microcontroller for verification against a secure database of registered voters. RFID ensures contactless, quick, and accurate identification, making it ideal for environments that demand security and speed. In the voting system, RFID plays a critical role in user authentication. Each voter is assigned a tag that is pre-registered with the election system. At the polling booth, the voter must scan their RFID card. Upon scanning, the system retrieves the tag's ID and compares it to the stored records to determine the voter's eligibility. If verified, the system proceeds to the next step—face recognition or confirmation through input devices. RFID prevents unauthorized access, eliminates duplicate entries, and minimizes human intervention, thus increasing system reliability.

Since it is contactless, it also improves hygiene and ease of use, especially in crowded or remote areas. Another major benefit of RFID is its ability to work without line-of-sight, unlike barcodes or magnetic stripe cards. This allows for faster processing of voters and reduces delays during elections. Additionally, RFID tags are difficult to duplicate, enhancing the security of the voting process. The integration of RFID with microcontrollers like Arduino allows seamless data transfer and automated decision-making. For instance, if a tag is invalid or not found in the database, the system can instantly alert the user and prevent access, all within milliseconds. Thus, RFID not only streamlines the authentication process but also strengthens the integrity and scalability of the voting system.

3.GSM (Global System for Mobile Communications)

GSM modules are devices that enable a microcontroller to communicate over a mobile network. They allow the system to send and receive messages, access data services, and even establish calls if necessary. In a voting system, GSM is used to send real-time alerts and notifications to voters, administrators, or security personnel. For example, when a vote is successfully cast or if unauthorized access is detected, the system can send an SMS to the relevant stakeholders. GSM modules operate using a SIM card, just like mobile phones, and can be programmed to send text messages via standard AT commands. The use of GSM in the proposed voting system greatly enhances transparency and security. Upon successful authentication and voting, the system can send a confirmation message to the voter's registered mobile number. This serves as proof that their vote was cast and helps build trust in the system. Similarly, in case of a failed authentication or suspected fraudulent activity, alerts can be sent instantly to the election officers. The GSM module thus functions as a communication bridge between the system and external parties, ensuring real-time monitoring and response. This reduces manual oversight and allows remote election management in decentralized locations. Moreover, GSM modules are relatively easy to interface with microcontrollers like the Arduino Nano. They communicate via serial connections and support functions such as message formatting, sending, and receiving, all through programmable code. The integration of GSM makes the system more robust, especially in rural or low-infrastructure settings where internet access may be limited. Since GSM relies on mobile networks, it can operate independently of broadband connections, providing a reliable backup channel for communication. Its role in the voting system is not just functional but also strategic, enabling real-time updates and enhancing user engagement through transparent information exchange.

4. Input Key (Keypad)

The input key, typically implemented as a matrix keypad, is a critical interface between the user and the system. In the proposed voting system, it allows users to interact with the system by entering PINs, selecting options, or confirming inputs. A 4x4 or 4x3 keypad configuration is commonly used, with each key sending a unique signal when pressed. The keypad is connected to the microcontroller, which scans the input lines to detect which key was pressed. This enables precise user input and verification, crucial for maintaining the security and efficiency of the voting process. The keypad in this system serves multiple functions. After scanning their identification card, a voter may be required to input a personal identification number (PIN) as an added layer of security. Alternatively, the keypad can be used to confirm the selection of candidates or menu options during the voting process. It offers a straightforward and user-friendly method of input, especially for users unfamiliar with touchscreen interfaces. The keypad can also be used by the system administrator to configure settings, perform system checks, or initiate emergency protocols if needed. One of the key advantages of using a keypad is its reliability and simplicity. Unlike touchscreens, which may be affected by environmental factors like moisture or temperature, physical keypads are robust and offer tactile feedback. They are also cost-effective and easy to maintain, making them ideal for large-scale deployment in diverse geographical regions. The combination of RFID, biometric verification, and keypad input creates a multi-layered security framework that ensures only authorized users participate in the voting process. Furthermore, keypad interactions can be logged for audit trails, contributing to the transparency and accountability of the election. In conclusion, the keypad is an essential component that enhances user interaction, security, and system versatility.

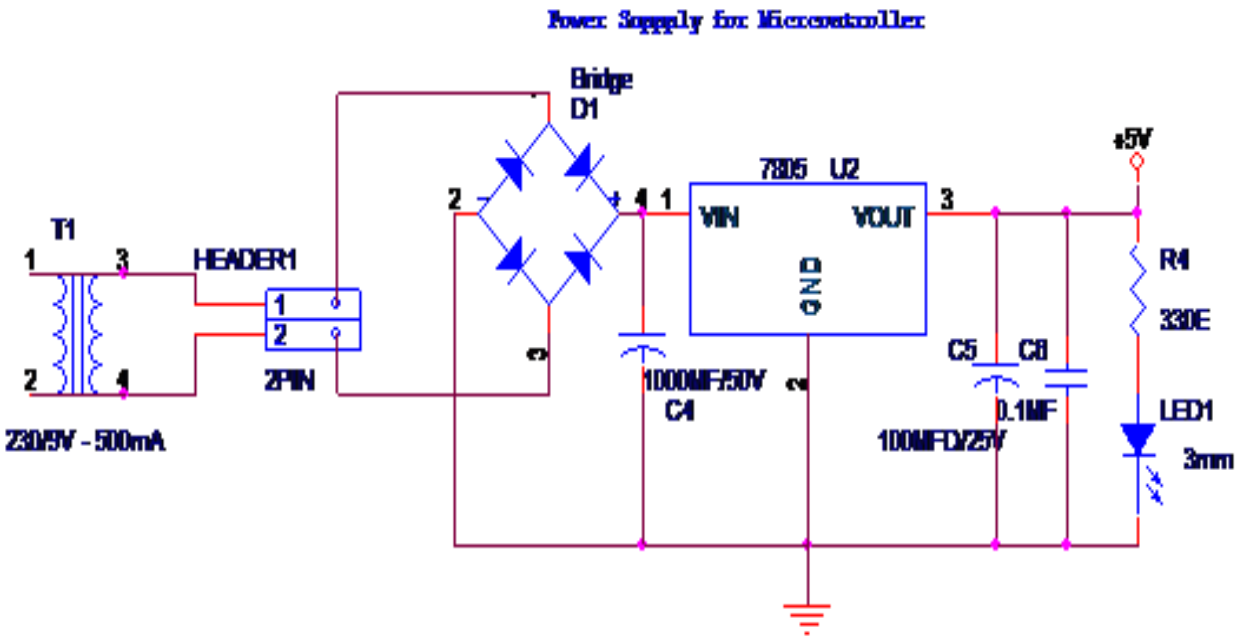
5. Power Supplies

A power supply (sometimes known as a power supply unit or PSU) is a device or system that supplies electrical or other types of energy to an output load or group of loads. The term is most commonly applied to electrical energy supplies, less often to mechanical ones, and rarely to others. This circuit is a small +5V power supply, which is useful when experimenting with digital electronics. Small inexpensive wall transformers with variable output voltage are available from any electronics shop and supermarket. Those transformers are easily available, but usually their voltage regulation is very poor, which makes then not very usable for digital circuit experimenter unless a better regulation can be achieved in some way. The following circuit is the answer to the problem.

Transformer

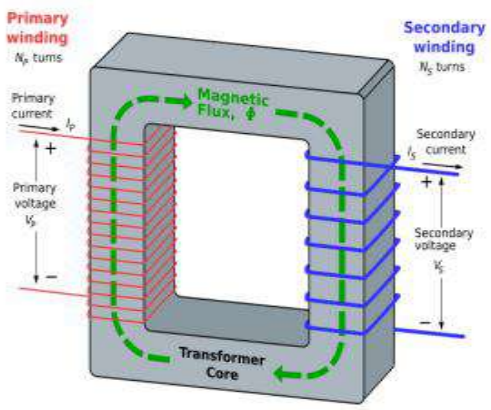
A transformer is a device that transfers electrical energy from one circuit to another through inductively coupled wires. A changing current in the first circuit (the primary) creates a changing magnetic field; in turn, this magnetic field induces a changing voltage in the second circuit (the secondary). By adding a load to the secondary circuit, one can make current flow in the transformer, thus transferring energy from one circuit to the other. The secondary induced voltage VS is scaled from the primary VP by a factor ideally equal to the ratio of the number of turns of wire in their respective windings: By appropriate selection of the numbers of turns, a transformer thus allows an alternating voltage to be stepped up by making NS more than NP or stepped down, by making it less. A key application of transformers is to reduce the current before transmitting electrical energy over long distances through wires. Most wires have resistance and so dissipate electrical energy at a rate proportional to the square of the current through the wire.

IJIRAE::International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 03, March 2026 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1303.43



Block diagram of power supply

By transforming electrical power to a high-voltage, and therefore low-current form for transmission and back again afterwards, transformers enable the economic transmission of power over long distances. Consequently, transformers have shaped the electricity supply industry, permitting generation to be located remotely from points of demand. All but a fraction of the world's electrical power has passed through a series of transformers by the time it reaches the consumer. Transformers are some of the most efficient electrical 'machines', with some large units able to transfer 99.75% of their input power to their output. Transformers come in a range of sizes from a thumbnail-sized coupling transformer hidden inside a stage microphone to huge gigavolt-ampere-rated units used to interconnect portions of national power grids. All operate with the same basic principles, though a variety of designs exist to perform specialized roles throughout home and industry. The transformer is based on two principles: first, that an electric current can produce a magnetic field (electromagnetism) and, second, that a changing magnetic field within a coil of wire induces a voltage across the ends of the coil (electromagnetic induction). By changing the current in the primary coil, one changes the strength of its magnetic field; since the secondary coil is wrapped around the same magnetic field, a voltage is induced across the secondary.



An ideal step-down transformer

A simplified an ideal step-down transformer design is shown in the above figure. A current passing through the primary coil creates a magnetic field. The primary and secondary coils are wrapped around a core of very high magnetic permeability, such as iron; this ensures that most of the magnetic field lines produced by the primary current are within the iron and pass through the secondary coil as well as the primary coil.

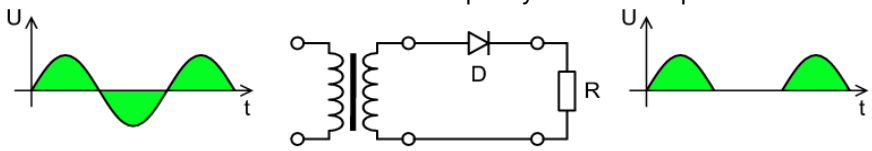
Rectifier

A rectifier is an electrical device that converts alternating current (AC), which periodically reverses direction, to direct current (DC), which flows in only one direction. The process is known as rectification. Rectifiers are used as components of power supplies and as detectors of radio signals. Mainly there are three types of rectifier i.e. half wave rectifier, full wave rectifier and Bridge Rectifier.

Half-wave rectifier

In half-wave rectification of a single-phase supply, either the positive or negative half of the AC wave is passed, while the other half is blocked. Because only one half of the input waveform reaches the output, mean voltage is lower.

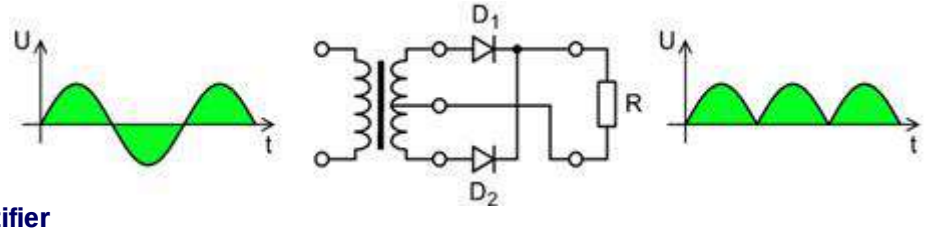
Half-wave rectification requires a single diode in a single-phase supply, or three in a three-phase supply. Rectifiers yield a unidirectional but pulsating direct current; half-wave rectifiers produce far more ripple than full-wave rectifiers, and much more filtering is needed to eliminate harmonics of the AC frequency from the output.



Half Wave Rectifier

Full-wave rectifier

A full-wave rectifier converts the whole of the input waveform to one of constant polarity (positive or negative) at its output. Full-wave rectification converts both polarities of the input waveform to pulsating DC (direct current), and yields a higher average output voltage. Two diodes and a center tapped transformer are needed.



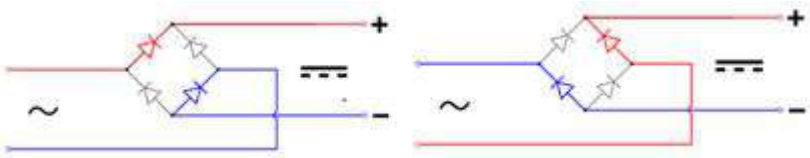
Full-Wave Rectifier

Bridge Rectifier

A diode bridge is an arrangement of four (or more) diodes in a bridge circuit configuration that provides the same polarity of output for either polarity of input. When used in its most common application, for conversion of an alternating current (AC) input into a direct current (DC) output, it is known as a bridge rectifier. A bridge rectifier provides full-wave rectification from a two-wire AC input, resulting in lower cost and weight as compared to a rectifier with a 3-wire input from a transformer with a center-tapped secondary winding. The essential feature of a diode bridge is that the polarity of the output is the same regardless of the polarity at the input.

Basic operation

According to the conventional model of current flow, current is defined to be positive when it flows through electrical conductors from the positive to the negative pole. In actuality, free electrons in a conductor nearly always flow from the negative to the positive pole. In the vast majority of applications, however, the actual direction of current flow is irrelevant. Therefore, in the discussion below the conventional model is retained. In the diagrams below, when the input connected to the left corner of the diamond is positive, and the input connected to the right corner is negative, current flows from the upper supply terminal to the right along the red (positive) path to the output, and returns to the lower supply terminal via the blue (negative) path.

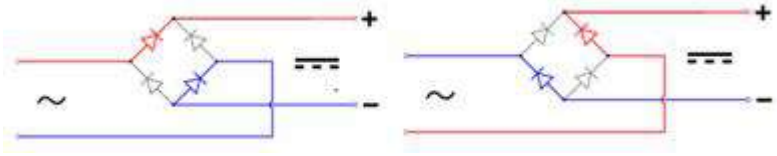


Operation of bridge rectifier

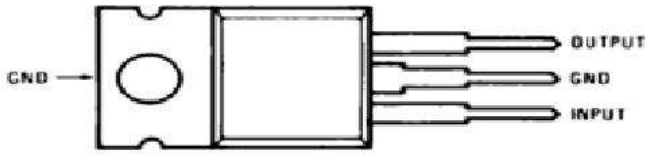
When the input connected to the left corner is negative, and the input connected to the right corner is positive, current flows from the lower supply terminal to the right along the red (positive) path to the output, and returns to the upper supply terminal via the blue (negative) path. In each case, the upper right output remains positive and lower right output negative. Since this is true whether the input is AC or DC, this circuit not only produces a DC output from an AC input, it can also provide what is sometimes called "reverse polarity protection". That is, it permits normal functioning of DC-powered equipment when batteries have been installed backwards, or when the leads (wires) from a DC power source have been reversed, and protects the equipment from potential damage caused by reverse polarity.

IC Voltage Regulators

Voltage regulators comprise a class of widely used ICs. Regulator IC units contain the circuitry for reference source, comparator amplifier, control device, and overload protection all in a single IC. Although the internal construction of the IC is somewhat different from that described for discrete voltage regulator circuits, the external operation is much the same. IC units provide regulation of either a fixed positive voltage, a fixed negative voltage, or an adjustable set voltage. A power supply can be built using a transformer connected to the ac supply line to step the ac voltage to desired amplitude, then rectifying that ac voltage, filtering with a capacitor and RC filter, if desired, and finally regulating the dc voltage using an IC regulator. The regulators can be selected for operation with load currents from hundreds of milliamperes to tens of amperes, corresponding to power ratings from milliwatts to tens of watts.



IJIRAE::International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 03, March 2026 https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1303.43



Top View

Three-Terminal Voltage Regulators

Figure shows the basic connection of a three-terminal voltage regulator IC to a load. The fixed voltage regulator has an unregulated dc input voltage, Vi, applied to one input terminal, a regulated output dc voltage, Vo, from a second terminal, with the third terminal connected to ground. For a selected regulator, IC device specifications list a voltage range over which the input voltage can vary to maintain a regulated output voltage over a range of load current. The specifications also list the amount of output voltage change resulting from a change in load current (load regulation) or in input voltage (line regulation). The series 78 regulators provide fixed regulated voltages from 5 to 24 V. Figure shows how one such IC, a 7805, is connected to provide voltage regulation with output from this unit of +5V dc. An unregulated input voltage V is filtered by capacitor C1 and connected to the IC's IN terminal. The IC's OUT terminal provides a regulated + 12V which is filtered by capacitor C2 (mostly for any high-frequency noise). The third IC terminal is connected to ground (GND). While the input voltage may vary over some permissible voltage range, and the output load may vary over some acceptable range, the output voltage remains constant within specified voltage variation limits. These limitations are spelled out in the manufacturer's specification sheets. There are two types of voltage regulator they are 78xx series and 79xx series.

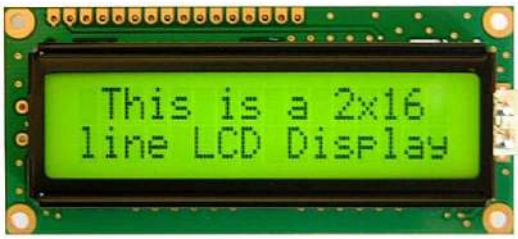
78xx series

There are common configurations for 78xx ICs, including 7805 (5 V), 7806 (6 V), 7808 (8 V), 7809 (9 V), 7810 (10 V), 7812 (12 V), 7815 (15 V), 7818 (18 V), and 7824 (24 V) versions. The 7805 is the most common, as its regulated 5-volt supply provides a convenient power source for most TTL components. Less common are lower-power versions such as the LM78Mxx series (500 mA) and LM78Lxx series (100 mA) from National Semiconductor. Some devices provide slightly different voltages than usual, such as the LM78L62 (6.2 volts) and LM78L82 (8.2 volts) as well as the STMicroelectronics L78L33ACZ (3.3 volts).

79xx series

The 79xx devices have a similar "part number" to "voltage output" scheme, but their outputs are negative voltage, for example 7905 is -5 V and 7912 is -12 V. The 7912 has been a popular component in ATX power supplies, and 7905 was popular component in ATX before -5 V was removed from the ATX specification.

6. LCD (LIQUID CRYSTAL DISPLAY)



LCD Display

LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits.

Based on the construction, LCD's are classified into two types. They are,

(i) Dynamic scattering type

(ii) Field effect type.

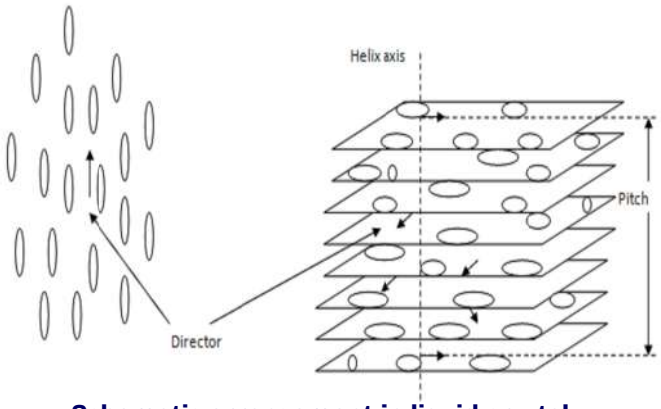
Dynamic scattering type

The construction of the dynamic scattering liquid crystal cell is shown in the fig. The display consists of two glass plates, each coated with tin oxide (SnO2) on the inside with transparent electrodes separated by a liquid crystal layer,5μA to 50 μA thick. The oxide coating on the front sheet is etched to produce a single or multi- segment pattern of characters, with each segment properly insulated from each other. A weak electric field applied to liquid crystal tends to align molecule in the direction of the field. As soon as the voltage exceeds certain threshold value, the domain structure collapses and the appearance is changed. As the voltage grows further, the flow becomes turbulent and the substance turns optically homogenous. In this disordered state, the liquid crystal scatters light. Thus, when the liquid is not activated, it is transparent. When the liquid is activated, the molecular turbulence causes light to be scattered in all directions and the cell appears bright. This phenomenon is called dynamic scattering

Field effect type

The construction of the field effect LCD display is similar to that of the dynamic scattering type, with the expectation that two thin polarizing optical filters are placed at the inside of each glass sheet. The LCD material is of twisted nematic type which twists the light (change in direction of polarization) passing through the cell when the latter is not energized.

This allows light to pass through the optical filters and the cell appears bright. When the cell is energized, no twisting of light takes place and the cell appears dull. for field effect cells LCD's require ac voltage supply. A typical voltage supply to dynamic scattering LCD's are normally used for seven-segmental displays.



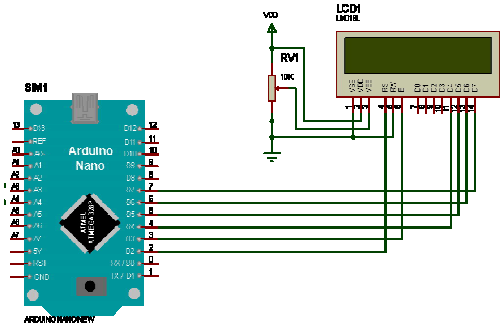
Schematic arrangement in liquid crystal

Features of LCD

Operating voltage range is 3-20V ac.
It has a slow decay time. Response time is 50 to 200 ms.
Viewing angle is 100 degree.
Invisible in darkness. Requires external illumination.
Life time is limited to 50,000 hours due to chemical graduation.

Advantages of LCD

The voltage required is small.
They have low power consumption. A seven segment display requires about 140 W (20 W per segment).



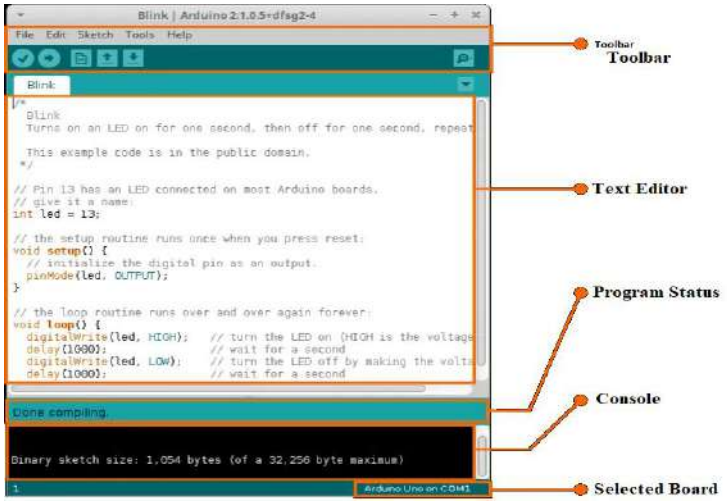
LCD interface with Arduino NANO

4.4 SOFTWARE DESCRIPTION

ARDUINO SOFTWARE (IDE)

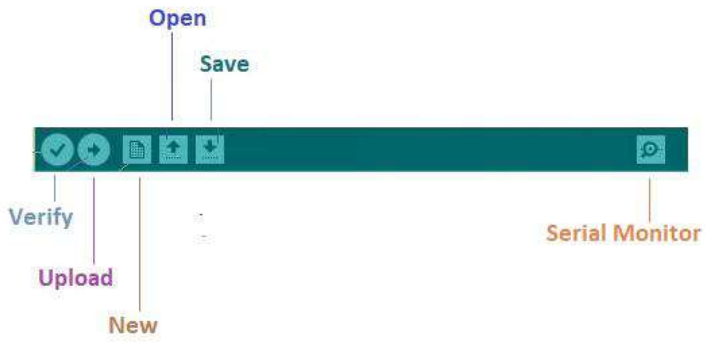
The Arduino Integrated Development Environment - or Arduino Software (IDE) - contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino hardware to upload programs and communicate with them.

Arduino IDE



Writing Sketches

Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension .ino. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Arduino Software (IDE), including complete error messages and other information. The bottom righthand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor.



Arduino IDE Tool Icon

Verify Checks your code for errors compiling it. Upload Compiles your code and uploads it to the configured board. See uploading below for details. Note: If you are using an external programmer with your board, you can hold down the "shift" key on your computer when using this icon. The text will change to "Upload using Programmer" New Creates a new sketch. Open Presents a menu of all the sketches in your sketchbook. Clicking one will open it within the current window overwriting its content. Save Saves your sketch. Serial Monitor Opens the serial monitor. Additional commands are found within the five menus: File, Edit, Sketch, Tools, Help. The menus are context sensitive, which means only those items relevant to the work currently being carried out are available.

File

New Creates a new instance of the editor, with the bare minimum structure of a sketch already in place. Open Allows to load a sketch file browsing through the computer drives and folders. Open Recent Provides a short list of the most recent sketches, ready to be opened. Sketchbook Shows the current sketches within the sketchbook folder structure; clicking on any name opens the corresponding sketch in a new editor instance. Examples Any example provided by the Arduino Software (IDE) or library shows up in this menu item. All the examples are structured in a tree that allows easy access by topic or library. Close Closes the instance of the Arduino Software from which it is clicked. Save Saves the sketch with the current name. If the file hasn't been named before, a name will be provided in a "Save as.." window. Save as... Allows to save the current sketch with a different name. Page Setup It shows the Page Setup window for printing. Print Sends the current sketch to the printer according to the settings defined in Page Setup. Preferences Opens the Preferences window where some settings of the IDE may be customized, as the language of the IDE interface. Quit Closes all IDE windows. The same sketches open when Quit was chosen will be automatically reopened the next time you start the IDE.

Edit

Undo/Redo Goes back of one or more steps you did while editing; when you go back, you may go forward with Redo.
Cut Removes the selected text from the editor and places it into the clipboard. Copy Duplicates the selected text in the editor and places it into the clipboard. Copy for Forum Copies the code of your sketch to the clipboard in a form suitable for posting to the forum, complete with syntax coloring. Copy as HTML Copies the code of your sketch to the clipboard as HTML, suitable for embedding in web pages. Paste Puts the contents of the clipboard at the cursor position, in the editor. Select All Selects and highlights the whole content of the editor. Comment/Uncomment Puts or removes the // comment marker at the beginning of each selected line. Increase/Decrease Indent Adds or subtracts a space at the beginning of each selected line, moving the text one space on the right or eliminating a space at the beginning. Find Opens the Find and Replace window where you can specify text to search inside the current sketch according to several options. Find Next Highlights the next occurrence - if any - of the string specified as the search item in the Find window, relative to the cursor position. Find Previous Highlights the previous occurrence - if any - of the string specified as the search item in the Find window relative to the cursor position.

Sketch

Verify/Compile Checks your sketch for errors compiling it; it will report memory usage for code and variables in the console area. Upload Compiles and loads the binary file onto the configured board through the configured Port. Upload Using Programmer This will overwrite the bootloader on the board; you will need to use Tools > Burn Bootloader to restore it and be able to Upload to USB serial port again. However, it allows you to use the full capacity of the Flash memory for your sketch. Please note that this command will NOT burn the fuses. To do so a Tools -> Burn Bootloader command must be executed. Export Compiled Binary Saves a .hex file that may be kept as archive or sent to the board using other tools. Show Sketch Folder Opens the current sketch folder. Include Library Adds a library to your sketch by inserting #include statements at the start of your code. For more details, see libraries below. Additionally, from this menu item you can access the Library Manager and import new libraries from .zip files.

Add File... Adds a source file to the sketch (it will be copied from its current location). The new file appears in a new tab in the sketch window. Files can be removed from the sketch using the tab menu accessible clicking on the small triangle icon below the serial monitor one on the right side o the toolbar.

Tools

Auto Format This formats your code nicely: i.e. indents it so that opening and closing curly braces line up, and that the statements inside curly braces are indented more. Archive Sketch Archives a copy of the current sketch in .zip format. The archive is placed in the same directory as the sketch. Fix Encoding & Reload Fixes possible discrepancies between the editor char map encoding and other operating systems char maps. Serial Monitor Opens the serial monitor window and initiates the exchange of data with any connected board on the currently selected Port. This usually resets the board, if the board supports Reset over serial port opening. Board Select the board that you're using. See below for descriptions of the various boards. Port this menu contains all the serial devices (real or virtual) on your machine. It should automatically refresh every time you open the top-level tools menu. Programmer For selecting a hardware programmer when programming a board or chip and not using the onboard USB-serial connection. Normally you won't need this, but if you're burning a bootloader to a new microcontroller, you will use this. Burn Bootloader The items in this menu allow you to burn a bootloader onto the microcontroller on an Arduino board. This is not required for normal use of an Arduino board but is useful if you purchase a new ATmega microcontroller (which normally comes without a bootloader). Ensure that you've selected the correct board from the Boards menu before burning the bootloader on the target board. This command also set the right fuses.

Help

Here you find easy access to a number of documents that come with the Arduino Software (IDE). You have access to Getting Started, Reference, this guide to the IDE and other documents locally, without an internet connection. The documents are a local copy of the online ones and may link back to our online website. Find in Reference this is the only interactive function of the Help menu: it directly selects the relevant page in the local copy of the Reference for the function or command under the cursor.

Sketchbook

The Arduino Software (IDE) uses the concept of a sketchbook: a standard place to store your programs (or sketches). The sketches in your sketchbook can be opened from the File > Sketchbook menu or from the Open button on the toolbar. The first time you run the Arduino software, it will automatically create a directory for your sketchbook. You can view or change the location of the sketchbook location from with the Preferences dialog. Tabs, Multiple Files, and Compilation. Allows you to manage sketches with more than one file (each of which appears in its own tab). These can be normal Arduino code files (no visible extension), C files (.c extension), C++ files (.cpp), or header files (.h). Before compiling the sketch, all the normal Arduino code files of the sketch (.ino, .pde) are concatenated into a single file following the order the tabs are shown in. The other file types are left as is.

Uploading

Before uploading your sketch, you need to select the correct items from the Tools > Board and Tools > Port menus. The boards are described below. On the Mac, the serial port is probably something like /dev/tty.usbmodem241 (for an Uno or Mega2560 or Leonardo) or /dev/tty.usbserial-1B1 (for a Duemilanove or earlier USB board), or /dev/tty.USA19QW1b1P1.1 (for a serial board connected with a Keyspan USB-to-Serial adapter). On Windows, it's probably COM1 or COM2 (for a serial board) or COM4, COM5, COM7, or higher (for a USB board) - to find out, you look for USB serial device in the ports section of the Windows Device Manager. On Linux, it should be /dev/ttyACMx , /dev/ttyUSBx or similar. Once you've selected the correct serial port and board, press the upload button in the toolbar or select the Upload item from the Sketch menu. Current Arduino boards will reset automatically and begin the upload. With older boards (pre-Diecimila) that lack auto-reset, you'll need to press the reset button on the board just before starting the upload. On most boards, you'll see the RX and TX LEDs blink as the sketch is uploaded. The Arduino Software (IDE) will display a message when the upload is complete, or show an error. When you upload a sketch, you're using the Arduino bootloader, a small program that has been loaded on to the microcontroller on your board. It allows you to upload code without using any additional hardware. The bootloader is active for a few seconds when the board resets; then it starts whichever sketch was most recently uploaded to the microcontroller. The bootloader will blink the on-board (pin 13) LED when it starts (i.e. when the board resets).

Libraries

Libraries provide extra functionality for use in sketches, e.g. working with hardware or manipulating data. To use a library in a sketch, select it from the Sketch > Import Library menu. This will insert one or more #include statements at the top of the sketch and compile the library with your sketch. Because libraries are uploaded to the board with your sketch, they increase the amount of space it takes up. If a sketch no longer needs a library, simply delete its #include statements from the top of your code. There is a list of libraries in the reference. Some libraries are included with the Arduino software. Others can be downloaded from a variety of sources or through the Library Manager. Starting with version 1.0.5 of the IDE, you do can import a library from a zip file and use it in an open sketch. See these instructions for installing a third-party library.

Third-Party Hardware

Support for third-party hardware can be added to the hardware directory of your sketchbook directory. Platforms installed there may include board definitions (which appear in the board menu), core libraries, bootloaders, and programmer definitions.

To install, create the hardware directory, then unzip the third-party platform into its own sub-directory. (Don't use "arduino" as the sub-directory name or you'll override the built-in Arduino platform.) To uninstall, simply delete its directory.

Serial Monitor

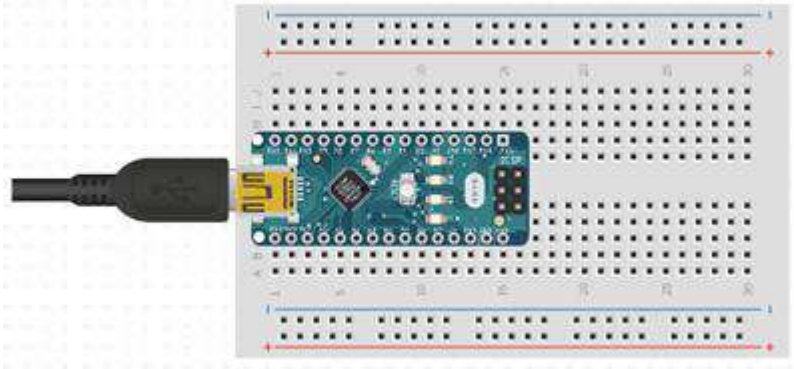
This displays serial sent from the Arduino board over USB or serial connector. To send data to the board, enter text and click on the "send" button or press enter. Choose the baud rate from the drop-down menu that matches the rate passed to Serial.begin in your sketch. Note that on Windows, Mac or Linux the board will reset (it will rerun your sketch) when you connect with the serial monitor. Please note that the Serial Monitor does not process control characters; if your sketch needs a complete management of the serial communication with control characters, you can use an external terminal program and connect it to the COM port assigned to your Arduino board.

Preferences

Some preferences can be set in the preferences dialog (found under the Arduino menu on the Mac, or File on Windows and Linux). The rest can be found in the preferences file, whose location is shown in the preference dialog. Boards The board selection has two effects: it sets the parameters (e.g. CPU speed and baud rate) used when compiling and uploading sketches; and sets and the file and fuse settings used by the burn bootloader command. Some of the board definitions differ only in the latter, so even if you've been uploading successfully with a particular selection you'll want to check it before burning the bootloader. Arduino Software (IDE) includes the built in support for the boards in the following list, all based on the AVR Core. The Boards Manager included in the standard installation allows to add support for the growing number of new boards based on different cores like Arduino Due, Arduino Zero, Edison, Galileo and so on.

STARTED WITH THE ARDUINO NANO

The Arduino Nano is a small, complete, and breadboard-friendly board based on the ATmega328P. It offers the same connectivity and specs of the UNO board in a smaller form factor.



Arduino NANO Interface

The Arduino Nano is programmed using the Arduino Software (IDE), our Integrated Development Environment common to all our boards and running both online and offline. For more information on how to get started with the Arduino Software visit the Getting Started page. Arduino Nano on the Arduino Desktop IDE If you want to program your Arduino Nano while offline you need to install the Arduino Desktop IDE To connect the Arduino Nano to your computer, you'll need a Mini-B USB cable. This also provides power to the board, as indicated by the blue LED (which is on the bottom of the Arduino Nano 2.x and the top of the Arduino Nano 3.0).

NANO Interfacing USB Types of Port

Open your first sketch

Open the LED blink example sketch: File > Examples >01.Basics> Blink.

Select your board type and port

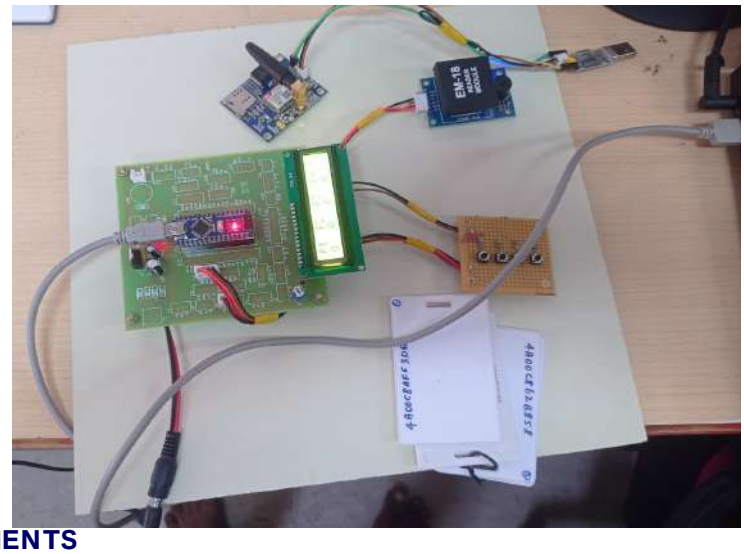
Select Tools > Board > Arduino AVR Boards > Arduino Nano.

NOTE: We have updated the Nano board with a fresh bootloader. Boards sold by us from January 2018 have this new bootloader, while boards manufactured before that date have the old bootloader. First, check that Tools > Board > Boards Manager shows you have the Arduino AVR Boards 1.16.21 or later installed. Then, to program the NEW Arduino NANO boards you need to choose Tools > Processor > ATmega328P. To program old boards you need to choose Tools > Processor > ATmega328P (Old Bootloader). If you get an error while uploading or you are not sure which bootloader you have, try each Tools > Processor menu option until your board gets properly programmed.

Select the NANO Processor Type : Select the serial device of the board from the Tools | Serial Port menu. This is likely to be COM3 or higher (COM1 and COM2 are usually reserved for hardware serial ports). To find out, you can disconnect your board and re-open the menu; the entry that disappears should be the Arduino board. Reconnect the board and select that serial port. Select Board Type: modules writtenin languages such as C, or use Py Py, a just-in-time compiler. C Python is also available, which translates a Python script into C and makes direct C-level API calls into the Python interpreter. An important goal of Python's developers is keeping it fun to use. This is reflected in the language's name a tribute to the British comedy group Monty Python and in occasionally playful approaches to tutorials and reference materials, such as examples that refer to spam and eggs (from a famous Monty Python sketch) instead of the standard for and bar. Python's initial development was spearheaded by Guido van Rossum in the late 1980s. Today, it is developed by the Python Software Foundation.

Because Python is a multiparadigm language, Python programmers can accomplish their tasks using different styles of programming: object oriented, imperative, functional or reflective. Python can be used in Web development, numeric programming, game development, serial port access and more. There are two attributes that make development time in Python faster than in other programming languages: Python is an interpreted language, which precludes the need to compile code before executing a program because Python does the compilation in the background. Because Python is a high-level programming language, it abstracts many sophisticated details from the programming code. Python focuses so much on this abstraction that its code can be understood by most novice programmers. Python code tends to be shorter than comparable codes. Although Python offers fast development times, it lags slightly in terms of execution time. Compared to fully compiling languages like C and C++, Python programs execute slower. Of course, with the processing speeds of computers these days, the speed differences are usually only observed in benchmarking tests, not in real-world operations. In most cases, Python is already included in Linux distributions and Mac OS X machines.

V.RESULTS & DISCUSSION



HARDWARE REQUIREMENTS

The implementation of the advanced voting system demonstrated significant improvements in terms of accuracy, security, and operational efficiency. The primary goal of integrating automated identification cards with live biometric verification was successfully achieved through the use of RFID cards and a real-time image matching system. During testing, the system consistently authenticated voters correctly, ensuring that only eligible individuals were allowed to cast their votes. The two-factor verification process eliminated the possibility of multiple voting or unauthorized access, which had been a recurring issue in traditional paper-based voting systems. The response time of the system was notably efficient. From the moment a voter scanned their identification card to the successful face verification and vote casting, the entire process took under 10 seconds per individual. This quick processing time helped in reducing long queues and wait times, which are commonly experienced in conventional voting setups. Furthermore, the system's automated logging of each action added an additional layer of transparency, making it easier for election officials to audit records and verify that the process was conducted fairly. Throughout various testing scenarios, the system showed a high level of stability and reliability. The RFID card reader accurately read all registered voter cards without failure, and the facial recognition module successfully authenticated individuals even under different lighting conditions. Cases of failed authentication were appropriately flagged by the system, prompting either manual inspection or re-attempt, without disrupting the process. This ensured that no ineligible vote was cast while maintaining user confidence in the voting procedure. In addition, the integration of a communication module allowed for real-time updates and alerts. Voters received confirmation messages after casting their votes, which added to the overall transparency and helped in keeping voters informed. In case of anomalies such as a mismatch in biometric data or invalid cards, the system could notify election officials immediately, enabling rapid intervention. This level of responsiveness adds a new dimension of control and accountability in the voting process. From a usability standpoint, the system was found to be intuitive for users of varying ages and technical knowledge. The keypad interface allowed users to confirm actions or enter a personal code when required, and the visual and audio indicators helped guide them through each step. This simplicity is particularly important for implementation in rural or technologically underserved areas, where ease of use is essential for adoption. One key discussion point is scalability. The modular architecture of the system, built around a compact microcontroller, allows it to be deployed in elections of different sizes, ranging from local councils to national-level voting. Since it does not rely heavily on internet connectivity and can function with basic electrical supply and GSM communication, it is well-suited for use in remote or infrastructure-limited regions.

VI. CONCLUSION AND FUTURE ENHANCEMENT

6.1 Conclusion

The project successfully demonstrates the design and implementation of a smart, secure, and reliable voting system that integrates radio-frequency-based identity verification with facial recognition to enhance the integrity and transparency of electoral processes.

By incorporating dual-layer authentication, the system significantly reduces the chances of fraudulent voting, such as impersonation and multiple voting attempts. It also streamlines the voting process by automating verification, reducing manual intervention, and improving overall speed and accuracy. The inclusion of a GSM-based communication module enables real-time updates and notifications, enhancing user awareness and trust in the system. Throughout the development and testing phases, the system proved to be efficient, user-friendly, and adaptable to various voting environments, from local body elections to larger-scale implementations. The RFID technology ensures that only registered voters can access the system, while face recognition ensures that the identity of each voter is accurately confirmed before allowing vote casting. This comprehensive approach makes the voting process more secure and accountable while offering a seamless experience for the voter.

6.2 FUTURE ENHANCEMENT

To further improve the system, several enhancements can be introduced. First, implementing cloud-based data storage and blockchain technology could ensure even higher levels of data integrity, transparency, and tamper-proof records. Second, integrating multilingual user interfaces and accessibility features such as audio guidance or support for visually impaired individuals can expand usability among diverse populations. The system can also benefit from more advanced artificial intelligence models that improve facial recognition accuracy under varying environmental conditions, such as different lighting or partial occlusions. In the future, incorporating a mobile voting extension with secure identity verification could allow remote voting for citizens who are unable to be physically present at polling stations, such as military personnel, senior citizens, or expatriates.

REFERENCES

1. S.Zhang, L.Wang and H.Xiong, "Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability", International Journal of Information Security, vol. 19, no. 3, pp. 323-341, Sep. 2019.
2. B.Shahzad and J.Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology", IEEE Access, vol. 7, pp. 24477-24488, Jan. 2019.
3. U.Jafar, M.J.A.Aziz and Z.Shukur, "Blockchain for Electronic Voting System—Review and open Research Challenges", Sensors, vol. 21, no. 17, pp. 5874, Aug. 2021.
4. P.M.Dhulavvagol, V.H.Bhajantri and S.G.Totad, "Blockchain Ethereum Clients Performance analysis considering E-Voting application", Procedia Computer Science, vol. 167, pp. 2506-2515, Jan. 2020.
5. K.M.Khan, J.Arshad and M.M.Khan, "Investigating performance constraints for blockchain based secure e-voting system", Future Generation Computer Systems, vol. 105, pp. 13-26, Apr. 2020.
6. R.Taş and O.O.Tanrıöver, "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting", Symmetry, vol. 12, no. 8, pp. 1328, Aug. 2020.
7. T.Ali Syed, A.Alzahrani, S.Jan, M.S.Siddiqui, A.Nadeem and T.Alghamdi, "A comparative analysis of blockchain architecture and its applications", IEEE Access, vol. 7, pp. 176838-176869, 2019.
8. P.Rani, V.Kumar, I.Budhiraja, A.Rathi and S.Kukreja, "Deploying Electronic Voting System Use-case on Ethereum Public Blockchain", 2022
9. A.Singh and K.Chatterjee, "SecEVS: Secure Electronic Voting System Using Blockchain Technology", 2018